

S. HRG. 110–113

**WILL REAL ID ACTUALLY MAKE US SAFER?
AN EXAMINATION OF PRIVACY AND CIVIL
LIBERTIES CONCERNS**

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MAY 8, 2007

Serial No. J-110-33

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

37–167 PDF

WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ARLEN SPECTER, Pennsylvania
JOSEPH R. BIDEN, Jr., Delaware	ORRIN G. HATCH, Utah
HERB KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	JON KYL, Arizona
RUSSELL D. FEINGOLD, Wisconsin	JEFF SESSIONS, Alabama
CHARLES E. SCHUMER, New York	LINDSEY O. GRAHAM, South Carolina
RICHARD J. DURBIN, Illinois	JOHN CORNYN, Texas
BENJAMIN L. CARDIN, Maryland	SAM BROWNBACK, Kansas
SHELDON WHITEHOUSE, Rhode Island	TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*

MICHAEL O'NEILL, *Republican Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	229
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania	3

WITNESSES

Carafano, James Jay, Assistant Director, Kathryn and Shelby Cullom Davis Institute for International Studies, and Senior Research Fellow, Douglas and Sarah Allison Center for Foreign Policy Studies, Heritage Foundation, Washington, D.C.	10
Gilbert, Allen, Executive Director, American Civil Liberties Union of Vermont, Montpelier, Vermont	6
Harper, Jim, Director, Information Policy Studies, The Cato Institute, Wash- ington, D.C.	8
Kephart, Janice, President, 9/11 Security Solutions, LLC, Alexandria, Vir- ginia	15
Schneier, Bruce, Founder and Chief Technology Officer, BT Counterpane, Minneapolis, Minnesota	12

QUESTIONS AND ANSWERS

Responses of James Carafano to questions submitted by Senator Leahy	31
Responses of Jim Harper to questions submitted by Senator Leahy	33
Responses of Janice Kephart to questions submitted by Senator Leahy	37
Responses of Bruce Schneier to questions submitted by Senator Leahy	43

SUBMISSIONS FOR THE RECORD

American Association of Motor Vehicle Administrators, Michael R. Calvin, Interim President & CEO, Washington, D.C., statement	46
Carafano, James Jay, Assistant Director, Kathryn and Shelby Cullom Davis Institute for International Studies, and Senior Research Fellow, Douglas and Sarah Allison Center for Foreign Policy Studies, Heritage Foundation, Washington, D.C., statement	56
Center for Democracy and Technology, Ari Schwartz, Deputy Director, state- ment	63
Electronic Privacy Information Center, Washington, D.C., statement	70
Gilbert, Allen, Executive Director, American Civil Liberties Union of Vermont, Montpelier, Vermont, statement and attachments	131
Harper, Jim, Director, Information Policy Studies, The Cato Institute, Wash- ington, D.C., statement and attachments	167
Information Technology Association of America, Arlington, Virginia, state- ment	186
Kephart, Janice, President, 9/11 Security Solutions, LLC, Alexandria, Vir- ginia	196
Minner, Hon. Ruth Ann, Governor, State of Delaware, Wilmington, Delaware, letter	231
Schneier, Bruce, Founder and Chief Technology Officer, BT Counterpane, Minneapolis, Minnesota, statement	234
Vermont Department of Motor Vehicles, Bonnie L. Rutledge, Commissioner, letter	238
Wall Street Journal: National ID Party, February 17, 2005	241

IV

	Page
Wall Street Journal—Continued	
Immigration Reality Check, May 4, 2005	243
Deputizing the DMV, July 25, 2005	245
Real ID Revolt, May 8, 2007	246

WILL REAL ID ACTUALLY MAKE US SAFER? AN EXAMINATION OF PRIVACY AND CIVIL LIBERTIES CONCERNS

TUESDAY, MAY 8, 2007

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 10:12 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Feingold, and Specter.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Good morning. I apologize to Senator Specter and to the witnesses for being late. We sometimes, as the late Senator Moynihan used to say, act like a Third World nation around here, with closing off streets for motorcades, usually for somebody who, if they would simply drive up in an ordinary car, nobody would even know who they are or care, but we have to have motorcades to attract attention. Unfortunately, we do it with a lot of our own officials more and more. This one stopped traffic for about 20 minutes. If I could have just left my car, I could have easily walked to the Capitol.

I recall when I was a law student here at Georgetown, one time up in the Capitol, I got on an elevator and stopped, and there was then-Vice President Lyndon Johnson and one agent with him. I stopped. He said, "Boy, are you getting on or off?" I said, "Well, I was getting on, Mr. Vice President." He grabbed me by the lapel and pulled me on, and he said, "Well, get on." I watched as he drove off. He was in a car with a driver, one agent, and that was it.

The other day I noticed the Vice President came up to lobby some of our colleagues, and between the motorcycles and all the others, I counted 38 vehicles. Somewhere we have gotten out of control.

I also recall—well, that is another story. I won't expand.

[Laughter.]

Chairman LEAHY. We are turning our attention to an issue of great concern to States and to those Americans who value their privacy in the face of the Federal Government's expanding role in their daily lives, and I thank our witnesses for being here. I especially thank Allen Gilbert from Vermont, who told me he drove by

early this morning the road to my own farm in Vermont and all looked peaceful.

I look forward to gaining a better understanding of the impact of the so-called REAL ID Act. Actually, that is something we should have done, the Congress should have done before they passed the Act. But too often we will pass acts and then find out afterward whether or not they make any sense. I do not think this does.

It was legislation forced through by the last Congress as an add-on to an emergency supplemental bill. I do not recall hearing objections to this sweeping substantive legislation being jammed into an emergency supplemental from those who this year were so critical of the important aspects of the U.S. Troop Readiness, or Veterans' Care, Katrina Recovery, or Iraq Accountability Appropriations Act. This bill would have provided for veterans care and Katrina relief and other needs in the emergency supplemental legislation that we passed last week and the President vetoed last week.

The REAL ID Act was attached to an emergency supplemental, with no hearings, no votes, but what it is, the Federal Government will be dictating how the States go about the business of licensing residents to operate motor vehicles. State motor vehicle officials will be required to verify the legal status of applicants, adding to the responsibilities of already heavily burdened State offices. And if anybody thinks it is going to be a walk in the park standing in line at your local motor vehicle department, if you think you wait there a long time just for routine things, you can imagine what this is going to be like.

While the Federal Government dictates responsibilities for what has traditionally been a State function—and adds layers of bureaucracy and regulation to effectively create a national ID card, and that is what it is—there is no help in footing these hefty bills. It is an unfunded mandate passed by the last Congress to add to the taxpayers of the States \$23 billion in costs.

The Wall Street Journal noted in an editorial—and I might note that the Wall Street Journal is not one of my biggest fans, but they noted in an approving editorial today that “REAL ID was always more about harassing Mexican illegals than stopping Islamic terrorists.” It was put in “in an effort to placate noisy anti-immigration conservatives amid the GOP’s poll-driven election panic.” And it was attached to a “must-pass military spending bill” without hearings or debates, and the President “made the mistake of signing it.”

Given my own concerns, I have joined with Senators Akaka, Sununu, and Tester to introduce a bill that would repeal this law. We could have had negotiations, which would have been completed, and would have rested in stronger requirements for identification documents by now had the REAL ID Act not been forced through. You know, we were trying to actually work out something that made some sense. That all came to a halt when we did this, Oh, well, just pass \$23 billion of extra taxes onto our States and let them do it.

We all know the critical importance of national security. But security measures have to be smart as well as tough. Any one of us who flies often knows that there are some security measures taken

that make sense, and others that look like window dressing for the sake of window dressing.

The reaction to the unfunded mandates of the REAL ID Act is a pretty good example of what happens when the Federal Government imposes itself rather than creating a partnership with the States.

In addition to the numerous stakeholders that I understand have made substantial comments, I hope that the DHS—a Department which has very real difficulties in just running itself and keeping itself secure—will pay close attention to the sentiments expressed by members of this Committee and by the Homeland Security and Governmental Affairs Committee, which held an oversight hearing on REAL ID in March. I think the days of Congress rubberstamping any and every idea cooked up by the administration are over. Let's see real solutions with demonstrable results before we throw away billions of dollars—or more accurately, push those costs onto the States—in the name of some vague claims of enhanced security.

I want to understand better the implications for individual privacy rights and national security of this law. I will put into the record the editorial from this morning's Wall Street Journal, Review and Outlook, "REAL ID Revolt."

[The prepared statement of Senator Leahy appears as a submission for the record.]

Senator Specter, again, I apologize to you. You were here on time. I was not.

STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Senator SPECTER. Thank you, Mr. Chairman. This hearing is part of the continuing efforts of the Judiciary Committee to strike an appropriate balance between national security and individual liberty and privacy. We all know the terrorist threat, and it is important to be able to identify people, to know who is doing what, including flying on airplanes, which posed the 9/11 catastrophe. But even the 9/11 hijackers had multiple identifications, so the question is: How do we have identification which can be checked?

REAL ID, for anybody who has not heard the expression, is real identification, that is, accurate identification. There have been tremendous objections raised already about this REAL ID from very diverse groups such as the American Conservative Union, at one end of the political spectrum; the American Civil Liberties Union, at the other end of the spectrum; and the National Organization for Women. These groups have a lot of people who are objecting to it. And it has quite a number of proponents in trying to deal with the issue of finding out who is who and what the problems may be.

The Department of Homeland Security has asked for comments as part of the rulemaking process and got thousands of comments. The Department of Homeland Security estimates it will cost 23—I want to be sure we have the zeros right, \$23 billion. As I thought about it, I wanted to check my notes to see that this was accurate. It is going to cost a lot of money for the States. Eleven States have filed resolutions in opposition, two States have opted out, 33 States

have moved ahead to comply. So there is a checkerboard of responses.

We are wrestling with the issue of immigration legislation. A prodigious amount of work has been put into that by many Senators sitting down for hours on end. Hard to believe you can find as many as 10 or 12 Senators who will sit for 2 hours to work on immigration, and one of the issues that we are struggling with there is, beyond securing borders, to have employers know who is legal and who is not legal. And we are wrestling with the costs of foolproof identification.

Then we have the issue about the citizens who are applying for a job. How can the employer be sure even citizens are what they claim to be—citizens? So that is a matter of enormous concern.

You come on a very busy day. You only see customarily the Chairman and the Ranking here because there are so many collateral duties, and I am going to have to excuse myself in a few minutes. We are trying to put together an immigration bill because the Majority Leader has given notice that it is going to be on the floor next Monday, and he is going to employ what is called Rule XIV to bypass the Committee. I am not sure that, Mr. Chairman, Senator Leahy, has been wise, because we have been doing a lot of wheel spinning on the meetings we have had. Last year, when I was Chairman and Senator Leahy—this is role reversal—we had in this room elongated meetings, but we hammered out a bill without going into all the details. And we met the deadline which we had, and the bill which we produced in the Senate may be our starting point under this Rule XIV procedure where the Committee does not act. But that decision was made thinking we could craft a bill which would be agreeable to all parties, and that may turn out to be wishful thinking to find anything that is agreeable to all parties in the U.S. Senate.

So we are wrestling with a tough issue with this REAL ID, and I appreciate the presence of the witnesses. We are going to try to find another Republican to come to participate in the hearing, but we will be watching your testimony very closely. We appreciate your inputs as we wrestle with this issue about how we identify people and still protect privacy.

One item that I noted of special concern is that REAL ID does not respect the rights of the Amish and the Mennonites, who wish not to have their pictures taken. They have the right not to have their photographs taken, rights recognized by the U.S. Supreme Court precedent and State law. And we need to respect people's rights, and that is another issue. Pennsylvania has quite a number, but we need to respect rights of Americans wherever they may reside.

So we have got some weighty issues here, Mr. Chairman. Senator Leahy has just shown me some identification, but I am prepared to vouch for him without even seeing identification.

[Laughter.]

Senator SPECTER. I have known him for 27 years in the United States, and our friendship goes back to 1970 when we were prosecuting attorneys, when we had real jobs.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

I was showing Senator Specter my Vermont driver's license, which does not have a picture on it. And I might say, which has nothing to do with this hearing—

Senator SPECTER. It is one of the few documents in the world which does not have Senator Leahy's picture.

[Laughter.]

Chairman LEAHY. We will invite them to the Leahy Center in Burlington. But, you know, all these things—the Amish and the Mennonites—all that should have been thought about before. This was just rammed down with no hearings or anything else, actually by the other body.

I may have mentioned what—Senator Specter spoke of immigration. He deserves the thanks of both Republicans and Democrats in the Senate for the enormous work he put into this in the past 2 years. I was privileged to work with him on that and helped us keep our quorums and get things moving, and Senator Specter—I am glad that the Democratic leader has made sure that he is involved in these meetings. I think we did get a good piece of legislation out here that can be our starting point, and I would hope that we would move forward on this.

I agree with President Bush—this will stop the presses, but I agree with him when he says he wants a comprehensive immigration bill. But I think that is what Senator Specter, under his leadership, put through last year. Well, let us try again.

Senator SPECTER. Thank you, Pat.

Chairman LEAHY. Lady and gentlemen, would you please stand and raise your right hand? Do you solemnly swear that the testimony you will give in this matter will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. GILBERT. I do.

Mr. HARPER. I do.

Mr. CARAFANO. I do.

Mr. SCHNEIER. I do.

Ms. KEPHART. I do.

Chairman LEAHY. We will hear from each of you. We will begin with Allen Gilbert from Vermont. He is the Executive Director of the American Civil Liberties Union of Vermont. He has been a leading voice in our State about the REAL ID's impact on our State and our way of life. He also served as President of the Vermont School Board Association. He lives not far from me in Vermont and traverses the dirt roads that go near my home.

Allen, you would be interested in knowing that years ago, when our oldest son, Kevin Leahy, who is now a lawyer in Montpelier, when he was in his early teens, he was asked by a reporter what kind of vehicle his father prefers during mud seasons on a dirt road. He said, "Dad prefers a rental vehicle for mud season."

He was a reporter, then city editor of the Vermont Herald, later served as assistant editor of the Sunday Rutland Herald Times, was a free-lance writer, taught writing at several Vermont colleges and American studies at a German university; a bachelor's degree in history from Harvard, a master's degree in education from the College of William and Mary.

Thank you very much for coming down. Please go ahead with your testimony.

**STATEMENT OF ALLEN GILBERT, EXECUTIVE DIRECTOR, THE
AMERICAN CIVIL LIBERTIES UNION OF VERMONT, MONTPE-
LIER, VERMONT**

Mr. GILBERT. My name is Allen Gilbert. I live in Worcester, Vermont—which is the next town over from Senator Leahy’s town, Middlesex—and I want to thank Chairman Leahy for having us here to testify.

People in Vermont have a lot of unanswered questions about REAL ID. Seldom have I encountered an issue that raises concerns among such a wide range of people. I can talk with a legislator about REAL ID, and she will point out that the National Conference of State Legislatures expresses misgivings about the program. I can talk with a member of the National Gun Owners in Vermont, and he will worry about Government intrusion. A member of an advocacy group for victims of domestic and sexual violence worries that REAL ID threatens protection programs for women and children.

The Ancient Order of Hibernians does not like REAL ID, and neither does the American Friends Service Committee. Earlier this year, the Government Operations Committee of the Vermont House of Representatives passed, unanimously, a resolution opposing REAL ID. The resolution was subsequently approved, also unanimously, by the full Vermont House. The longest-serving member in the Vermont House sits on the Government Operations Committee. Rep. Cola Hudson was born when a fellow Vermont Republican, Calvin Coolidge, was in the White House. Representative Hudson simply shook his head “No” when REAL ID was described in his committee.

Our Motor Vehicles Commissioner testified in another legislative committee about the “re-enrollment process” required by REAL ID. Everyone will have to visit a DMV office with proper documents. For some people in Vermont, that means a long trip. And when they get to the DMV office, our commissioner said, “The jokes about waiting in line at DMV are no longer going to be jokes but reality.”

Long-time residents are going to feel like suspects when they are required to report and show their papers. Our commissioner noted that her father is 82 years old. He has had a driver’s license for years. It is going to be hard to tell him, she said, that he has to prove his identity before he can get his license renewed. People in Vermont pride themselves on being part of tightly knit communities. Questioning who someone is, is seen as a sign of unfriendliness.

Birth records in Vermont are kept by town clerks. The clerks—some of whom are part-time—are already in a frenzy over the thought of complying with the myriad requests for records they are going to get because of REAL ID.

A State senator, who in his other life runs a construction company and races stock cars, said, “I am not sure if it is the budgetary concern or the privacy concern or the nightmare it is going to create that concerns me most about this.”

A series of data breaches this winter in Vermont led people to wonder about the security of stored data anywhere. DMV officials acknowledge that there are hundreds of unauthorized attempts

daily to get at the department's information data base. Increasingly, Vermonters are worried that too much data is being collected about too many things. It is not just a sense that privacy is eroding. Vermonters are worried that their identities will be stolen by identity thieves.

Vermonters are pretty responsible people. We generally step up to the plate when asked to do the right thing. But many people are not so sure that REAL ID is the right thing. It seems too big, too expensive, and too centralized.

Mr. Bruce Schneier, who is going to speak a bit later, is here. I heard him speak last year, and one of the things that he said has really stuck with me. He said that security is an equation, with one side being what you are giving up and the other side what you are getting in return. I am afraid that with REAL ID we are giving up too much and not getting much, if anything, in return.

REAL ID is going to cost the States a lot of money. The cost in Vermont is now estimated at around \$8 million. That is a pretty substantial expenditure for us. Some of our State senators want to raise license fees and to call the increase a "congressional REAL ID tax."

The cost, the implementation, the risk of identity theft—these things worry Vermonters. Vermonters are not convinced that REAL ID is a program that will make Americans safer.

On behalf of the ACLU, its 53 affiliates and half a million members, I urge you to mark up and move S. 717, the Akaka-Sununu-Leahy-Tester bill. That bill would replace REAL ID with sensible, cost-effective driver's license standards. The problems with REAL ID would be fixed, and the standards could be achieved in a cooperative fashion with State officials, Federal Government agencies, and privacy and civil liberties experts.

Thank you for the opportunity to testify this morning.

[The prepared statement of Mr. Gilbert appears as a submission for the record.]

Chairman LEAHY. Thank you very much.

Mr. Gilbert describes the Vermont attitude. I know a couple of the people he referred to. I would consider them among our most conservative folks back home. But about the only thing I ever kept from the press written about me and actually framed was a sidebar to a profile in one of our major publications. And as I said, I live on a dirt road. This summer we will have had this old tree farm in the family for about 50 years, a great deal of acreage and fields that have to be hayed, and there is an adjoining farm family through successive generations who watch over the place.

The whole thing went like this: It was a Saturday morning. A New York Times reporter in an out-of-State car sees a farmer sitting on the porch. He says, "Does Senator Leahy live up this road?" The farmer replied, "Are you a relative of his?" He said, "No." "Well, are you a friend of his?" "Well, not really." "Is he expecting you?" "No." "Never heard of him."

[Laughter.]

Chairman LEAHY. That is the kind of attitude we have.

Now, Jim Harper is the Director of Information Policy Studies at the Cato Institute. As Director of Information Policy Studies, he focuses on the unique problems of adapting law and policy to the

problems of the Information Age. He is a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. He is the editor of Privacilla.org, a web-based think tank devoted exclusively to privacy, and he maintains online Federal spending resource WashingtonWatch.com. He holds a J.D. from Hastings College of the Law.

Mr. Harper, thank you for taking the time to be here today.

**STATEMENT OF JIM HARPER, DIRECTOR, INFORMATION
POLICY STUDIES, THE CATO INSTITUTE, WASHINGTON, D.C.**

Mr. HARPER. Thank you, Mr. Chairman. Thank you for having this hearing, and thank you for having me here to testify on REAL ID.

In my opinion, the REAL ID Act is a dead letter. All that remains is for Congress to declare it so. At this point, my understanding is that eight States will not implement REAL ID. That means that States that do will not even get the benefits alleged from REAL ID. States that implement it at this point will be throwing good money after bad.

The proposed regulations issued by the Department of Homeland Security on March 9th, on which comments close today, help to reveal that REAL ID is a loser. It costs more to implement than it would add to our Nation's security protections.

In my written testimony, I have submitted a risk-based analysis of REAL ID, something DHS did not do, but I used DHS estimates to show that REAL ID's returns, its security returns, at best are 88 cents on the security dollar that we ask the States to spend on this.

It is important to understand that an identity system does not apply a fixed identity to everyone. It causes our attackers, it causes opponents, to change their behavior, to engage in fraud, to avoid identity systems entirely. It is rather trivial, frankly, for a committed attacker of any kind to work around or to break an identity system like we are talking about in REAL ID. So the security benefits are not there.

Because they are here to defend themselves, I will talk a little bit about the arguments made by proponents of REAL ID. I do so in the spirit of friendship, and I do not think anybody puts forward their arguments in bad faith. But the proponents of REAL ID essentially hew to two schools.

One is the "just do it" school. It is a law. If we just spend a lot more money on it, we will have this thing, and we will get whatever we are supposed to get from it. In a paper issued last week, my colleague, Jim Carafano, said, "Identity is one of the cornerstones of a free society." And I dropped my spoon into my Cheerios when I read that, because identity is also one of the cornerstones of a totalitarian society. The important question is who controls it, and I think it is much more important to decide whether Government should control identity or whether individuals in the United States should control identity. So I think it was an unthoughtful assertion in that case.

It also caused me some regret to see that the Heritage Foundation is supporting the expenditure of \$23 billion in a funded or un-

funded mandate on the States. It is an organization that I have an affinity for and a past affiliation with.

The other school is the “do over” school: If we could just go back and do it over again, maybe we could have done something using REAL ID to stop the terrorists. I know I sound a little glib in calling this the “do over” school, and we would all like to be able to go back and change the outcome on that day. But the “do over” school, if we could just go back and do it again, is not serious security argumentation. We are trying to design systems to secure our country going forward in the future, and the ability to go back and change things so that everyone would like it we do not have. So we have to think in terms of identity systems and how future attackers would avoid them or break them.

You have heard from Allen Gilbert the privacy and convenience and expenditure concerns that are shared throughout the country. The regulations issued by the Department of Homeland Security essentially punted on the most important technology, security, and privacy problems. Of utmost importance, in my opinion, the DHS proposal also lays the groundwork for systematic tracking of Americans, law-abiding Americans, based on their race.

Though the Department of Homeland Security failed to fix it in the regs, I do not think this is the agency's fault. And, again, people at DHS are working on these problems in good faith. Regulations cannot make this law work, and neither can delay. The real problem is the REAL ID law itself.

As you mentioned, Mr. Chairman, there are meritorious bills pending in the Senate and House to repeal REAL ID and restore the identification security provisions that were passed in the 9/11 Commission-inspired Intelligence Reform and Terrorism Prevention Act. Congratulations to you, Mr. Chairman, for being an original cosponsor of this legislation.

These bills would be improved on the margin if they were to chart a path to Government use of emerging digital credentialing systems—systems that are diverse, competitive, and privacy protective. You can get security without surveillance. It is a couple generations down the road using very advanced technologies, but it is possible to do. We can have these identification and credentialing systems. Governments can be users of them. REAL ID is the ugly alternative to getting it right.

Thank you very much.

[The prepared statement of Mr. Harper appears as a submission for the record.]

Chairman LEAHY. Well, thank you, and I could not help but think, in listening to your testimony on the costs, I could think of some ways we could spend that \$22 billion that would actually improve our security. And I understand Dr. Carafano will disagree with me, although I must say that I consider it a privilege to have Dr. Carafano testify before us. He is the Assistant Director for the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow at the Douglas and Sarah Allison Center for Foreign Policy Studies. Dr. Carafano is an accomplished and recognized historian and teacher. He is an assistant professor at the U.S. Military Academy at West Point. He also taught at Mount St. Mary College. He served as a fleet professor at the U.S.

Naval War College. He is a visiting professor at the National Defense University, I would also note with pride, at Georgetown. He graduated from West Point, has a master's degree and a doctorate from Georgetown, as well as a master's degree in strategy from the U.S. Army War College.

Doctor, as I mentioned to you privately, I appreciate you taking the time to be here, as you have every time we have asked you to come before this Committee.

STATEMENT OF JAMES JAY CARAFANO, ASSISTANT DIRECTOR, KATHRYN AND SHELBY CULLOM DAVIS INSTITUTE FOR INTERNATIONAL STUDIES, AND SENIOR RESEARCH FELLOW, DOUGLAS AND SARAH ALLISON CENTER FOR FOREIGN POLICY STUDIES, HERITAGE FOUNDATION, WASHINGTON, D.C.

Mr. CARAFANO. Thank you, Mr. Chairman. I appreciate this opportunity, and I have submitted a statement for the record.

I just want to make three points very quickly: why this is an incredibly important issue, what are the options, and then what should be done.

I do believe that identity is the cornerstone of a free society because we make a presumption in a free society that our citizens are acting lawfully and they should be left to go on their way. And we all know democracy works best in small communities because we have the trust and confidence of knowing each other. That is why Vermont is such an outstanding State.

But we live in a large, diverse society, and a verified identity is critical to having that freedom of movement, and that is why criminals so assiduously go after these documents and try to undermine them. And that is why it is so important to retain the credibility of identity documents in a free society. So we have three options.

One is we can do nothing. We can continue in the Wild West that we have had over the last decades where we have seen billions of dollars be lost every year to identity theft through fraud, theft, counterfeiting, and other types of criminal and malicious activities.

The alternative is we can do a national ID. We could try to create a single document that everybody in the country has to have. I think that is a wildly impractical, a wildly unnecessary, and, quite frankly, a wildly unachievable goal. And I think it is a ridiculous notion to think that we want to take authority and power away from the States, that federalism is not the right solution to making this society safe, free, and prosperous.

And the third alternative is we can do something reasonable, and I think what is implied by the REAL ID Act is something reasonable. It is voluntary programs for States that want to have their citizens have the privilege of presenting a credential for a Federal purpose. It is not a national identity card. It does not create new data bases. It does not give the Federal Government more information about our citizens than it has now. It does not put the Federal Government in charge of issuing or managing these programs. And it does not have to be an unfunded mandate and an unfair burden on the State.

So what should we do? And just let me kind of briefly click off my to-do list.

One is I do not think there is a legitimate constitutional issue here that needs to be adjudicated.

Second is I do not think that there is any kind of congressional legislative remedy required to fix the law.

Third is I think that rules can be fairly articulated and adjudicated under the system and that reasonable practices can be negotiated between the States and the Federal Government.

Fourth is I certainly think that adequate privacy protections can be implemented in the system and to meet the national standards required under the REAL ID Act.

And, fifth, I think we can fairly institute this system in a reasonable timeline. I think it is certainly appropriate that the Federal Government pay its fair share. I think it is a terrible idea that moneys to implement REAL ID come out of homeland security grants. It is simply robbing Peter to pay Paul. We have national requirements out there to raise our disaster and response preparedness systems in this country. If REAL ID is going to become a reality and a serious thing, it should have its own separate appropriations. And I think we should have a targeted strategy here. I think there are many States that are already virtually compliant with REAL ID, and I think we should focus our resources and our attention on the States that are closest to complying, also border States that want to use the REAL ID credential as a border-crossing card. Because I think once we have demonstrated the advantages of REAL ID, quite frankly, there will be a land rush for States to rush to implement this thing.

We should be very clear, and I will just say this in conclusion. This is obviously not a panacea. There is no identity credentialing system in the universe that is going to provide you 100 percent security. Every identity system at some point is going to be undermined or compromised. It is not a silver-bullet solution to fraud, theft, or counterfeiting. But there obviously is some security value in having national standards to which credentials that are presented for a Federal purpose all meet. And I do think—and I would dispute the economic analysis. I do think at the end of the day the value of national standards, the economic benefits and the reduction in threat and common security threats justifies the costs, and I think, quite frankly, the implementation costs have been severely overinflated and are unrealistic.

With that, Mr. Chairman, I thank you for the opportunity to be here today.

[The prepared statement of Mr. Carafano appears as a submission for the record.]

Chairman LEAHY. I would note that on the cost still it is an unfunded mandate to the States, and I think you would agree with that at this point. Yes or no?

Mr. CARAFANO. Mr. Chairman, I would agree that at this point there is not a reasonable agreement between the States and the Federal Government as to what the Federal Government's fair share is and how that should be implemented. So I do think that—

Chairman LEAHY. Well, no reasonable agreement insofar as the President has put zero in his budget for it. One would tend to think that, he being the decider, it is the position of the Federal Government that you are going to get zero.

Mr. CARAFANO. I agree, and I think that is just flat wrong. There should be a separate appropriation to implement REAL ID, and the Federal Government should pay its fair share.

Chairman LEAHY. We will go to Mr. Schneier in a second, but, you know, I worry. I see in the press today that Dulles Airport where I fly out almost every week to Vermont and go through the usual search—shoes off, belt off. I saw a woman who was berated for having a tiny little thing of hand purifier in her bag because she did not have it in a larger plastic bag, even though it was well within the amount, but she was berated for doing anything so foolish and threatening to the security of the United States. You see a 90-plus-year-old woman, having taken her shoes off, and then being told she can put them back on, and she explained she cannot put them on. The nurse usually does it at the home, and they say, “Well, it is your problem.” On more than one occasion, I have gone over and put the shoes back on. I see TSA losing so much of our identity, and today in the paper they said you can buy for \$100 a year some special ID to zip you through once you give them all kinds of background on yourself and fingerprints and everything else.

I have no intention of buying one of those. I will stand in line, go through the same things that others do, because I cannot trust them to keep the information they get on me. DHS, which is a dysfunctional agency in many, many ways, at least some who are waiting for the recovery from Katrina a couple years later might say, “Why should we trust you with it?” But I am going to give you plenty of time to answer that, and also, we will keep the record open for all the statements and also keep the record open, as you know, afterwards, if you have heard something somebody has said and you have not had a chance to respond to it, you will be given a chance for the record.

Mr. Schneier is an American cryptographer, computer security specialist, and a writer. He is the author of several books on computer security and cryptography. He is the founding chief technology officer at BT Counterpane. He has a master’s degree in computer science from American University, a bachelor of science degree in physics from the University of Rochester. Before Counterpane, he worked at the United States Department of Defense and then AT&T Bell Labs.

Mr. Schneier, thank you very much for taking the time to come here this morning.

STATEMENT OF BRUCE SCHNEIER, FOUNDER AND CHIEF TECHNOLOGY OFFICER, BT COUNTERPANE, MINNEAPOLIS, MINNESOTA

Mr. SCHNEIER. Thank you, Senator Leahy. I want to say that I am here as a security technologist and expert and not under the auspices of BT Counterpane. I have a statement from the Electronic Privacy Information Center for the rulemaking for the DHS, signed by 21 security experts. I would like to add that to the record.

Chairman LEAHY. Without objection, it will be part of the record.

Mr. SCHNEIER. My problem with REAL ID is it does not do what it claims to do. Most people think of ID cards basically as small,

rectangular pieces of plastic that include our name and our picture. But an ID card is part of the very complex security system, and once you start looking at the entire system, you realize that REAL ID is much more complicated and much less secure and much less valuable than its proponents say.

What really matters is not how it is used by the hundreds of millions of people who have it, but how it fails, how it can be abused by those who want to subvert it and want to get things that the ID should prevent.

First off, REAL ID will be forged. Every ID card ever invented has been forged. The new \$20 bill was forged even before it hit the streets. Money has a limit. You are not going to spend more than \$20 to forge a \$20 bill. A REAL ID card is an incredibly valuable piece of ID, so the value to forge it is much greater. And, paradoxically, by making a REAL ID, by making a single ID card, you increase the likelihood of forgery by making it more likely that the bad guys will spend more money to forge it.

REAL ID has problems in the sign-up process. You can never produce an ID card that is more secure than the breeder documents needed to get one. So if you look at the ways you would get a REAL ID, if those documents are easier to forge than a REAL ID, people will do that.

REAL ID will not prevent people from getting legitimate cards by bribing DMV clerks. This happens regularly. Some of the 9/11 terrorists did that. A hard-to-forge REAL ID, more stringent standards to get one will not protect us from someone basically being bribed to erroneously issue one.

But the biggest security risk is the data base. REAL ID requires a massive Government data base. DHS says that it is not one Government data base; it is 53 small ones. I think that is a red herring. Interconnected separate data bases are the same as one data base. You know this when you go on the Internet, when you look at Google. That is one data base.

This is a grave security risk. Senator Leahy, you just mentioned that last week the TSA lost 100,000 identities—not of us—of TSA employees, and this demonstrates how difficult it is for us to secure data bases. This I think is a bigger deal than the press is making it out. The identities of sky marshals are on this list. I think there are some grave security concerns here.

It was mentioned, I think by Mr. Gilbert, the problem of the identity requirements and address requirements for domestic abuse survivors. I think this is a big risk also for judges. My father is a judge in New York, and having his address on his ID is a security concern for him.

REAL ID also increases the risk of identity theft. There is a lot of talk about how it will decrease the risk. It actually will increase the risk.

First off, most identity theft is not based on people forging a piece of plastic. Identity theft is done electronically, and a single credential is a one-stop shop for identity thieves. We are more secure from identity thieves when we have multiple different credentials, when stealing one does not get you everything. The more things a single ID is used for, the greater at risk we are; the more value it is for someone to try to steal it and the more he can do

with it once he steals it. And if you think it is no fun when some criminal impersonates you to your bank, wait until some terrorist impersonates you to the TSA. That is going to be so much less fun.

Again, even if you can magically solve all these problems, even if you can make the ID work, REAL ID will not help us against terrorism. There is a myth in this country that if we could just identify people, we would know who they are, we know what they do. That is wrong. Identity does not map to intentionality. And if you want an idea of how identity-based security does not work, look at the no-fly list. The no-fly list is the one example of identity-based security that most of us come into contact with, and we know it does not work. It does not catch anybody, and it just harasses innocent people.

I was on the Diane Rehm show a couple of years ago, and there was a DHS person and we were debating this. And he said, you know, "When you are sitting on a plane, you want to know the identity of the person sitting next to you." And I said, "Well, that is not true. I want to know if he is going to blow up the aircraft. If he is not going to blow up the aircraft, I do not care who he is. And, honestly, if he is going to blow up the aircraft, I do not care who he is either." It is not the identity. It is the intentionality.

If you look at what we have done to help airport security, it is reinforcing the cockpit door, and it is teaching passengers how to fight back. It is not identifying who they are.

So I think REAL ID is a waste. As a taxpayer, I think \$23 billion is too much.

Thank you.

[The prepared statement of Mr. Schneier appears as a submission for the record.]

Chairman LEAHY. Thank you. You were talking about TSA making mistakes. Normally, the most senior member of this Committee is Senator Kennedy, and he was stopped about nine or ten times getting on a flight he has been taking for 40 years back to Boston because he is on a no-fly list.

Now, I have kidded Senator Kennedy about these Irish terrorists, they all look alike.

[Laughter.]

Chairman LEAHY. Dr. Carafano is chuckling because he knows of my Italian heritage. But, I mean, that is how ridiculous it is. He even had the President call him and apologize. He said, "Look, I do not want an apology. Just get me off the darn list." We have had a year-old child have to get a passport to prove they are not a 40-year-old suspected terrorist. Catholic nuns. I have to be careful when I recount some of my days in Catholic grade schools and high schools about whether some of them probably qualified as terrorists, but I do not think that it would be fair to lump them into this terrorist thing.

So, you know, you see mistakes being made there all the time. I do not feel any safer when I see Colin Powell in line in an airport and taking his shoes off and his belt off and being wanded and searched, especially when the person who is going to be cleaning the airplane while it is there is not getting anywhere near that kind of search, and the person who is alone in the airplane for about 20 minutes before you board and could put any kind of a

bomb on board that plane does not get the kind of security that General Powell or former Vice President Mondale, former Vice President Quayle, former Vice President Gore, and others do.

But I digress, and our next witness will be Janice Kephart. She is the President of 9/11 Security Solutions. She served as a counsel to the National Commission on Terrorist Attacks upon America, otherwise known as the 9/11 Commission. She is a key author of the 9/11 Commission staff report, "9/11 Terrorist Travel." She continues to work with the Canadian Embassy, international organizations, and top administration officials in an effort to pursue the implementation recommendations sought by both the 9/11 Commission and born of her own work.

Prior to her work on the Commission, she served as counsel to the Senate Judiciary Subcommittee on Terrorism, Technology, and Government Information, worked extremely hard on this Committee and knows the Committee well. And she is a graduate of Duke University and Villanova School of Law.

Ms. Kephart, thank you for taking the time to be here.

STATEMENT OF JANICE KEPHART, PRESIDENT, 9/11 SECURITY SOLUTIONS, LLC, ALEXANDRIA, VIRGINIA

Ms. KEPHART. Thank you, Chairman Leahy. It is an honor to be before you as an alum of the Committee that prepared me so well for my work on the 9/11 Commission. I appreciate very much this Committee's continued interest and effort in the 9/11 Commission recommendations, including the issue of identity document security that REAL ID addresses head-on.

I am here in my own capacity today, but I would like to remind you that the 9/11 Commission gave high marks for passing REAL ID legislation, and former Commissioner and Secretary of the Navy John Lehman had an op-ed in this morning's Washington Post in support of REAL ID. I am also happy to be one who speaks with the 70 percent of Americans who, in a very recent Zogby poll, are in favor of REAL ID driver's licenses.

To summarize where REAL ID stands today, every State DMV has taken at least a couple of steps toward REAL ID implementation. Forty-eight States and D.C. are checking Social Security numbers. Twenty check legal status. Three States are sharing vital events digitized records, and four

more are about to come online. Alabama, New York, and Texas are considered innovators in REAL ID compliance. In addition, at least 23 State legislatures have bills supporting REAL ID in some manner. And there are passed bills in favor of REAL ID as well in States like Kansas and Michigan.

The REAL ID law is based on the States' own exceptionally detailed post 9/11 work in establishing best practices to fix the State driver's license system that was known to generate neither secure IDs in content or production.

The critical question of this hearing—Will REAL ID actually make us safer?—is absolutely the correct question to ask. And the answer, in my opinion, an unequivocal yes, by assuring greater national and economic security, public safety, and privacy. If REAL ID is implemented, individual Americans' identities are less likely to be stolen, their children safer from underage drinking and driv-

ing, and as the Fraternal Order of Police has stated, a cop on the beat is more likely to know who is being encountered.

Last Wednesday, Subcommittee Chairwoman Feinstein held an excellent hearing on terrorist travel in this room whose theme was that secure IDs are essential for assuring people are who they say they are at our borders. REAL ID helps us do this within our borders. By looking at all the ways yesterday, today, and in the future as to how terrorists, counterfeiters, and criminals do their work.

The 9/11 hijackers, we need to remember, assimilated into the U.S. by attaining 17 driver's licenses from Arizona, California, and Florida and 13 State-issued IDs, including the 7 they fraudulently acquired in Virginia. Like other criminals and terrorists, the 9/11 hijackers then used those IDs for the purpose of renting cars, obtaining living quarters, and opening bank accounts. At least six hijackers total presented State-issued IDs on the morning of 9/11 to help look like Americans and board aircraft. The pilot who flew into the Pentagon had four IDs from four different States, and the Pennsylvania pilot had three IDs and an unverifiable ID when stopped for speeding 2 days prior to 9/11. The officer that stopped him needed an identity to associate with information, but he could not verify the ID, he could not verify the identity, and thus had no information to associate with it.

The 9/11 final report terrorist travel recommendations called for "setting standards for issuance of State IDs and designing a comprehensive screening system that sets common standards." The 9/11 Commissioners' 2005 final report gave Congress a really good mark for passing REAL ID, but cautioned "States' compliance needs to be closely monitored."

What has become unfortunate, in my opinion, is that myths and misinformation continue to abound about REAL ID, and let me address the most critical ones.

First, REAL ID is not a mandate. It preserves States' rights, letting States choose whether to comply or not. States are making that decision now. A mandate is a requirement, and REAL ID is not that.

Chairman LEAHY. Ms. Kephart, I will give you added time for this. Would you add that if it says that you are not going to be able to go into Federal buildings, citizens of your State cannot go into Federal buildings or board airplanes without it, do you still feel that is not a mandate?

Ms. KEPHART. It is not a mandate, sir, when you do not actually require the State to do it.

Chairman LEAHY. You just cannot fly or go into Federal buildings.

Ms. KEPHART. Well, what DHS has said is that they will just require—they will work with the States to provide another set of requirements. But DHS could answer that question.

Chairman LEAHY. Which they have not done.

Ms. KEPHART. I believe that will come out in the rules, sir. The ending date is today.

Second, REAL ID does not create a national data base. It does actually just the opposite. It keeps data flows to defined fields of information regarding Social Security information, birth and driv-

ing records, and other checks, with only the originator of the data capable of holding it and keeping it.

Third, REAL ID does not invade privacy. The current REAL ID Notice of Proposed Rulemaking makes recommendations for best practices States should employ to protect privacy, and they have put a lot of effort into that. These best practices are hefty. They build on the Commercial Driver's License Information System and the National Driver Register—data bases created in 1986 and serving 45 States. In 20 years of operations, there have been no complaints at all about intrusions on privacy or identity theft from either of those data bases. One reason why is the 1994 Driver's Privacy Protection Act which protects driver data. Also worth mentioning is that the ITAA, the Information Technology Association of America, yesterday issued a report stating that REAL ID protects privacy beyond what exists now. They represent the folks who do this work for a living.

Fourth, REAL ID does not create a national ID card. It avoids a national ID card. States use and control their own issuance processes, including meeting or exceeding REAL ID minimum standards.

In conclusion, to make REAL ID a reality requires more than just the Federal Government or the States can do alone. It requires a partnership. It also requires recognition that securing U.S. physical and economic integrity is not just a Federal responsibility. It is everyone's responsibility. Not implementing REAL ID simply keeps us right where we are, which is vulnerable. What we need now is to deal with what we have, make it work, and provide the real seed money necessary to help States comply with REAL ID. It is resolution of this issue that gets us closer to secure IDs sooner rather than perhaps never.

Thank you, Mr. Chairman.

[The prepared statement of Ms. Kephart appears as a submission for the record.]

Chairman LEAHY. Would you feel that the Federal Government should pick up the tab on this?

Ms. KEPHART. The Federal Government needs to do its share, sir, absolutely.

Chairman LEAHY. And what is its share?

Ms. KEPHART. Its share is the seed money to get the States started.

Chairman LEAHY. What is seed money—5 percent, 2 percent of the total—

Ms. KEPHART. Sir, I am not an economist to figure that out, but it is whatever the combination of DHS and OMB says the States need to get started. States have to maintain their own DMVs anyway, so what REAL ID needs to do is help them do what they—beyond what they would do anyway for achieving best practices to what REAL ID requires. And whatever that difference is is what the Federal Government should supply.

Chairman LEAHY. What State do you live in?

Ms. KEPHART. I am from Pennsylvania originally. I live in Virginia now.

Chairman LEAHY. Good luck when you are standing in line.

Ms. KEPHART. I would be happy to for my country, sir.

Chairman LEAHY. All of us would, if it really made our country safer, just as I am sure I would feel that we were doing a great deal for the country when we watch former Vice Presidents and former Secretaries of State and former Chairmen of the Joint Chiefs of Staff having to take their shoes off and everything else, knowing that that is making us safer.

Senator Feingold?

Senator FEINGOLD. Thank you, Mr. Chairman, very much for your great courtesy in letting me go ahead of you in the questions, and thanks to all the witnesses for their testimony on this important topic.

Mr. Harper and Mr. Gilbert, there has been a lot of discussion about the immense cost to State DMVs of implementing the REAL ID Act, but I have heard less about the burden on other types of record keepers which will be expected to verify identity documents as a part of the driver's license issuance process. Take birth certificates, which for most Americans who do not have passports are going to be the only proof of identity they can provide under the DHS regulations.

Birth certificates are issued by any of a number of local and State entities, and many birth certificate records are not electronic. Yet somehow all the State DMVs are going to have to verify with the issuing entity every birth certificate that is presented as proof of identity. I know this is going to be an issue in Wisconsin, where it is apparently going to cost approximately \$25 million to digitize and match all the birth, marriage, and death records in the State.

Can you expand on what vital records offices are going to need to do in order to comply with REAL ID and what sort of costs they can be expected to incur? And can you comment on whether this is a good idea to begin with? Mr. Gilbert?

Mr. GILBERT. Senator, Vermont has no vital records office in the sense that most States do. Birth certificates are kept in town clerks' offices, which are literally sometimes part of a person's home. So there often is not even security for these kinds of documents, and the authenticity of a birth certificate, I have been told, from Vermont is being questioned by more and more States because of the lack of security. But that is the way it has been done in Vermont for many, many years.

One of my sons was born in Vermont, and his birth certificate is kept by the town clerk of Berlin, Vermont. That is where the hospital where he was born is located. My other son was born in Germany. His birth certificate is on file with the U.S. Department of State. And for us to get a copy of his birth certificate, or for him to get a copy of it, I think he has to make application and wait—I do not know how long—until he gets a copy of the birth certificate.

But those are two examples of procedures that I think are going to be difficult for some people to be able to carry through on when they go to a DMV, and then the DMV is going to have to certify that the birth certificate from the Berlin, Vermont, town clerk's office as well as the U.S. Department of State birth certificate are accurate. That is going to require a lot of verification.

Senator FEINGOLD. Mr. Harper?

Mr. HARPER. Well, it is a foresighted question that I do not think has a good answer yet, because the local public records offices have yet to really get together and figure out what this problem is. The first wave of debate about REAL ID has been when State legislators recognized the cost to them of doing this. The next wave comes when the local offices, like Mr. Gilbert talked about, are asked to digitize or put online records that they have kept in drawers in their basements and hidden away.

In addition to the costs of doing that, the huge logistical problems with doing that, there are the security concerns with doing that. It is quite secure and quite private to have a paper document in a remote office somewhere. It is inefficient, but that inefficiency gives you security.

When these documents are scanned, when they are put online, when the scanned images and the information from them are in data bases, that is much more efficient, but it is much less secure. And I think people have yet to think about that dimension of the problem.

It is rather easy to put forward a pilot program and say, well, this pilot has suffered no breaches, there have been no complaints about this pilot program. The commercial driver's license system is an example where there are approximately 13 million commercial driver's licenses out there in the system. There is a difference in kind, not degree, from going to 13 million to going to 250 million, which include not just truck drivers but Senators, judges, officials of all kinds, and, for that matter, Paris Hilton. That is a system that is not secure the way a small system dealing with a relatively different class of people would be.

I have a shoebox in my apartment with business cards in it. It has never been breached. But if I put gold in it, it might be breached, and that is the kind of difference we are talking about.

Senator FEINGOLD. In that vein, REAL ID appears to be on its face simply a new system for issuing identification cards and driver's licenses. But I, too, am concerned that REAL ID will ultimately create a system used for a variety of other purposes that many people would find troubling, such as tracking Americans' movements and activities. And I see nothing in the proposed regulations limiting this type of use of the REAL ID cards and associated data bases. Am I right to be concerned about that? And what other potential consequences might arise? Mr. Harper?

Mr. HARPER. I do serve on the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. We had a meeting recently where Ann Collins, the Registrar of Motor Vehicles from the State of Massachusetts, spoke, and she said, "If you build it, they will come." What she meant by that is that if you compile deep data bases of information about every driver, uses for it will be found. The Department of Homeland Security will find uses for it. Every agency that wants to control, manipulate, and affect people's lives will say, "There is our easiest place to go. That is our path of least resistance."

So mission creep is the quick summary to this problem. If you build it, they will come. So I think it is very important to keep that in mind.

I will note, by the way, that the Department of Homeland Security's Privacy Committee is submitting comments to the DHS in its rulemaking, and the most important part of it to me—I think they took great care to offer helpful, constructive comments—but the most important part is at the outset the DHS Privacy Committee declined to endorse REAL ID as being an effective or appropriate program to put in place.

Senator FEINGOLD. Mr. Schneier, I understand that there have been numerous incidents in recent years of DMVs being broken into or DMV employees taking bribes to issue fraudulent licenses. Do those kinds of incidents remain a problem? And what do they suggest about the success of the REAL ID Act in securing driver's licenses?

Mr. SCHNEIER. Well, what it says is that secure identity systems are much more complicated than REAL ID, and certainly when you look at the system, you have to look at the mechanisms to get the card, what happens when you lose a card. And, you know, it is the breeder documents. You talk about the expense and convenience, but it is also the security. That would look at the ethics and how well trusted the people who issue the licenses are. You also have to look at the verification procedures. We were talking about the data bases and who has access to them. You do not have to worry about the data base itself, which should be accessible from police cars, airline check-in stations, schools, from wherever it is being used. Also, you have to think about the shadow data bases. Whenever you build a credential like this that is so valuable and so useful, there will be a shadow data base collected by the data brokers, that when you present your card at a hotel or at a bar, it will be scanned, and that data will go in the shadow data bases. Suddenly, what starts out as a simple data base becomes even bigger.

So, yes, I would worry about not only the clerks issuing them, I would worry about the clerks who are putting those birth certificates online. If it is cheaper to bribe them than it is to bribe a DMV clerk, you are going to do that.

If you want to subvert the system, you have to look at the weakest link, and just REAL ID is so incredibly complicated. There are so many links.

I put a diagram in my written testimony, which unfortunately I could not really put up on a screen, to try to lay out all the different ways there are security vulnerabilities in the system. And I think it is much more complicated than really a lot of people are thinking.

Senator FEINGOLD. OK. Mr. Gilbert and Mr. Schneier, identity theft is obviously a growing problem. Many people are concerned about the many recent security breaches of private and Government data bases containing sensitive personal information. Wouldn't the information gathered as part of REAL ID implementation also be vulnerable to these types of breaches? Mr. Gilbert?

Mr. GILBERT. This has been a big concern to people in Vermont because there has been a series of data breaches of Government data bases in our State just this past winter, and there were some legislative hearings held on this. Our Department of Motor Vehicles commissioner was asked the same question in testimony before one of the legislative committees, and she acknowledged that there

are over—there are several hundred attacks daily on their data base trying to get at the information in the DMV system.

She feels that their system is secure, but I think what Mr. Schneier is pointing out is true, that when you up the ante of the value of the information, the people who want that information are going to try harder and harder and do more and more to try and get at it. And I have become convinced that building a secure system is just very, very difficult, that there has got to be another way to do this. And I do not think we have found that quite yet.

Senator FEINGOLD. Mr. Schneier?

Mr. SCHNEIER. Mr. Harper has already said that there is security in keeping records offline, that there is inherent security of making them hard to get to. They are hard to look at, and they are hard to change.

Putting records online as part of REAL ID I think will make us less secure against identity theft because now data is more accessible, and it is also easier for someone to change.

In a lot of ways, REAL ID does not affect identity theft because identity theft is not based on a piece of plastic. It is based on electronically impersonating you via a website to a bank. What it does affect is it centralized credentials, and we are safer because an identity thief can go after only one thing—one bank account, one broker age account—and attacking one does not get you the other. And if REAL ID moves to its logical conclusion, where it becomes the single ID used for all sorts of things, if you read the DHS rule-making, that is what they are looking for. Then we are at increased risk of identity theft because now there is one document that can be stolen, which is the keys to everything.

It is really paradoxical. We are more secure from criminals through distributed identity. The fact that you could open up your wallet and you have a dozen different cards and each one does one thing and not just one card, that is what makes us safer.

Senator FEINGOLD. Thank you for your answers. I have to leave now, so I am just going to very briefly recess—I do not need to. The Chairman arrives.

Thank you, Mr. Chairman.

Chairman LEAHY. Speaking of Vermont, we had a group of Vermonters who stopped by, and I stepped out for a moment for that.

Mr. Gilbert, let us start with you. I have expressed—and I understand and I appreciate Dr. Carafano's and Ms. Kephart's views to the contrary, but I am concerned about the Federal Government basically taking over State DMVs. In fact, we have to protect our personal information. We also have to have national security. I am not sure they have to be exclusive by any means.

We know from what we have seen that had there been better use of the information we had, 9/11 could have been avoided. But I worry that the steps, those things that could make us vulnerable, are steps that are not being taken.

When you talk to other Vermonters about this, from your testimony—and I know you refer to the construction business. I know the others you are talking about. You have gone through a cross-section of Republicans, Democrats, across the political spectrum. Is there any one aspect more than others that people object to?

Mr. GILBERT. I think it is the privacy aspect that people are most concerned about. The money aspect is important to a legislator who is trying to find a couple million dollars to fix a bridge in his or her town. But I think the privacy aspect is something that just simply rankles Vermonters. And I think it rankles people in many other States around the country. There have been numerous resolutions and some binding legislation passed opposing REAL ID, and a good deal of that is based on a sense that REAL ID is going to violate privacy in a way that is not going to give us the security that has been promised.

And I think when people look at that kind of equation, they say it is simply not the way to go; we need another way to get at this problem of standards for driver's licenses.

Chairman LEAHY. You know, it is interesting on privacy. I have always had a listed home phone number. I had it when I was a prosecutor. I have it now. Most people will not call me at home. They figure that if I get a chance to be at home with my family, they are going to give me privacy, and it is kind of the way we are. But I worry more than just kind of the feelings we have in our State. I also worry that the information given can get lost. We have seen the VA in a colossal act of incompetence lose material with our personal information, the Department of Agriculture do the same thing. TSA has had material with backgrounds on people stolen out of their headquarters. Most recently, the Department of Agriculture posted people's Social Security numbers online. It has been almost mind-boggling, the data losses in this administration. But a lot of big companies have done it, too. T.J. Maxx is an example. We had one major bank who just simply shipped by commercial airline all of the personal information of their customers to go off to a storage thing, and it got lost. They cannot find where it went.

Now, I assume that their executives probably fly in private planes, and they are not used to having luggage lost. Any one of us who flies commercially, as I do and you do, knows that that actually happens. And it got lost, and they said, "Oops, sorry."

Let me ask also, you mentioned domestic violence groups. Tell me why the concern there.

Mr. GILBERT. The concern is that the victim of domestic sexual violence often wants to protect her residence, her identity in the sense of where she lives. She has a fear of physical attack. And Vermont is one of, I think it is about 20 States that currently offers a program where victims can use a post office box that actually is run by our Secretary of State's office, and mail, for example, can be delivered there, and the person can pick her mail up that way.

One of the problems with even the Department of Homeland Security's recognition of this problem is they have a fix in place for States like Vermont that already have a program, but for all the other States that do not have a program, it is not clear how identity could be protected in this way. And the victim advocates that I talk to in Vermont are really concerned about this.

Chairman LEAHY. Thank you. Let me ask this—Dr. Carafano?

Mr. CARAFANO. Sir, I think it is a perfect example of a fixable problem, why the rulemaking process is so important. Of course,

the easiest fix on this is for someone that has been a victim of domestic violence abuse or a judge or a Federal prosecutor or anyone that does not want their legal residence on the front face of their identity credential is to have a post office box. And I think that within the rulemaking process, that is an easy fix.

The law enforcement community does not need to see your address on the front of your identity credential. What they want to know is that you are you, that is primarily your full legal name, your date of birth, and your driver's license number. If they need to get your legal address, they can obtain that from other means.

So I do think that this is one that is not a show stopper in any way, shape, or form. It is an absolutely totally legitimate concern that can be addressed intelligently through the rulemaking process.

Chairman LEAHY. Well, I do note that I have a listed home phone number, both here in the Washington area and in Vermont, and it does not have a street address on it.

Mr. CARAFANO. And I do not think there is anything in REAL ID that should preclude people from wishing to have their post office box on the front of their credential.

Chairman LEAHY. I do not want my post office box on there. After all, I received one of the two deadly anthrax letters that I was supposed to open. It was sent to me. It was so deadly that two people who touched the outside of the envelope I was supposed to open died. I am not too eager to have my post office box there, which I do have. I get all my mail in a post office box. I am not too eager to have that known.

Mr. CARAFANO. There is no way it precludes somebody from getting your address and mailing you an evil thing, so that—

Chairman LEAHY. Nothing gets mailed to my home. Ever since they tried to kill me with a letter, it goes through a specialized screening area.

Let me ask you this, and I am going to ask this of each one of you. The Washington Post ran an editorial this morning by former Navy Secretary John Lehman supporting the law. Mr. Lehman argued that the REAL ID law will not result in a Federal data base.

A simple question of each of you: Do you agree with that?

Mr. GILBERT. I do not agree with that for the same reason when I go online and type in something in Google, I am essentially tapping into one integrated data base made up of thousands of other data bases around the world.

Chairman LEAHY. Mr. Harper?

Mr. HARPER. I do not agree with that.

Chairman LEAHY. Dr. Carafano?

Mr. CARAFANO. I absolutely agree with that. There is a significant distinction between a single centralized data base that does not have any firewalls, any intrusion protections, any kind of protocols, and integrated data bases where you can put in firewalls, you can put in intrusion detection devices, you can set up screening and all kinds of protocols to make sure of that. That is what we do with—because we live in a world of integrated data bases. If your argument is let us not have any integrated data bases because that is an unacceptable privacy concern, then this economy and this society is simply going to cease to function. It is a distinction with a significant difference.

Chairman LEAHY. So you agree this will not result in a Federal data base.

Mr. CARAFANO. This simply does not create a new national data base. Absolutely. There is no question about that.

Chairman LEAHY. Mr. Schneier?

Mr. SCHNEIER. I think it is a semantic dodge. There are lots of single data bases that have firewalls and IDSs. There are lots of single data bases that look like distributed data bases. There are distributed data bases that look like single data bases. How you implement it and how it is presented are completely orthogonal. This will result in a large Government data base, Federal or State. It will be accessed by both, so I am not convinced that is a difference that makes a difference.

What it does is it makes a single—it is a one-stop shop for the data, and that is what is important. And who writes the check I think is secondary, and exactly how the computer scientists build the computers and the networks is also secondary.

Chairman LEAHY. Ms. Kephart?

Ms. KEPHART. Well, I think it is a slam dunk, probably, what I will answer on that. Of course, I agree with former 9/11 Commissioner Lehman. In my testimony I have a chart. It is part of a paper that I released in April, and that chart shows the differentiated data bases that are checked.

Chairman LEAHY. So you agree that this would not be—

Ms. KEPHART. This is not a Federal—

Chairman LEAHY. This would not result in—

Ms. KEPHART.—data base. The data—

Chairman LEAHY.—a Federal data base. That—

Ms. KEPHART. OK. The data goes through—

Chairman LEAHY. That is a question—let me ask this next question. He asserts that the law is an unfunded mandate and that Congress should step up and fully fund the real costs that this essential program will impose on the States. Now, that is assuming that we do not change the program and it goes through as it was slipped into this appropriations bill.

I am going to ask each one of you: Do you agree with Mr. Lehman's assertion that this is an unfunded mandate and that Congress should step up and fully fund the real costs that this essential program imposes on the States? Mr. Gilbert?

Mr. GILBERT. I do not think Congress should fund any program that in the end is not going to be able to accomplish what the program is intended to do. If we could come up with a different program where we had cooperation with State and Federal officials, there was a chance for civil liberties and privacy experts to be involved, then I think it would be appropriate for the Federal Government to help the States pay for this.

Chairman LEAHY. Mr. Harper?

Mr. HARPER. It is an unfunded mandate, and it should not be funded because it should not be implemented.

Mr. CARAFANO. I do believe Congress should pay its fair share of implementation of the system. I think people in States have a right—many of these States have antiquated systems which are providing no protections. We talked a lot about commercial data. There is more data on us in the commercial sector than the Gov-

ernment has, and there are many best practices and excellent practices in the commercial sector to safeguard data, and the notion that we should expect—not hold our Government up to at least the standards of best practices in the commercial sector is just wrong.

Chairman LEAHY. Did T.J. Maxx follow those best practices?

Mr. CARAFANO. Again, sir, I did not say everybody in the commercial sector, but there are best practices out there that are in the commercial sector that are protecting data, and the notion that we should give our Governments a bye and not then at least safeguard our data as good as the people in the commercial sector is simply wrong.

Chairman LEAHY. Did the United States Department of Veterans Affairs follow that best practice?

Mr. CARAFANO. Again, sir, we should expect Government to do the right thing, and we should expect value for service. I mean, I think—I do not think—

Chairman LEAHY. We expected the Government to respond to Katrina and—

Mr. CARAFANO. I do not think that is a unreasonable requirement to expect our Government to do what the commercial sector can do in legitimately protecting data if they do the right thing. I mean, this is ridiculous to think—

Chairman LEAHY. Yes, I—

Mr. CARAFANO.—that we should have State that should be allowed—

Chairman LEAHY. I agree with—

Mr. CARAFANO.—to have 19th century systems that make their citizens incredibly vulnerable and that they do not provide a minimum level of protection. I think that is unreasonable. I think it is unconscionable.

Chairman LEAHY. I was not aware that in the 19th century we were issuing too many driver's licenses. But, Dr. Carafano, you know, we expect them to do that. But until they can prove they can do it, that worries me. When they—

Mr. CARAFANO. And—

Chairman LEAHY. May I finish, please?

Mr. CARAFANO. Yes, sir.

Chairman LEAHY. If it is OK with you. If the Department of Agriculture posts online people's Social Security numbers, sure, we can say we expect that it is part of the administration—the administration is strong on security, applaud them for saying the right things. But when they start releasing that online, that is not doing the right thing. When you cannot even secure computers inside TSA, it kind of makes you wonder. That is what I am saying.

We may well agree if we are going to have this, of course, there should be best practices. You and I agree on that. But so far, this administration, just like a lot of our major corporations and banks, has not demonstrated the best practices. We know it is best practices to be able to set up ATM machines where they cannot steal your ID. They are showing on television how easy it is because they have not set up such best practices to prevent the theft of your identification at ATM machines.

Mr. CARAFANO. Senator, every one of the criticisms that was mentioned here today exists in the systems as they currently exist

today. So if we do nothing, all the vulnerabilities that were mentioned here still exist there and persist. The notion is that if we do not create national standards, if we do not demand more from our Governments, they are never going to perform that. And I just think it is—the notion that somehow we are going to make progress by saying do nothing I think is just—it just does not make any sense. And that is why—

Chairman LEAHY. Just so we do not—

Mr. CARAFANO.—I think it is important for the Federal Government to pay its fair share to do the right thing.

Chairman LEAHY. OK. Just so we do not forget my yes-or-no question 15 minutes ago, Mr. Schneier, do you agree with Mr. Lehman's assertion that this is an unfunded mandate and that Congress should step up and fully fund the real costs?

Mr. SCHNEIER. I definitely think this an unfunded mandate. As a taxpayer, though, I do not want you to step up and pay the real costs because I am not getting the real benefit.

Now, I think you have been a little unfair to T.J. Maxx and the VA and the DHS because those are the ones that have made the news recently, but these breaches happen every single day.

Chairman LEAHY. Oh, I understand that, and in mentioning that, I just mention that because I think people understand, having seen it, that breaches happen every day, absolutely.

Mr. SCHNEIER. But the lesson in that is that this is hard to do. I mean, we can talk about best practices, but in reality, it is very, very hard to keep this data secure. And when you look at the system, the problem is not how do we make the IDs better, but the problem is we are relying on ID-based security.

There was a notion in the beginning, privacy versus security. That is a false dichotomy. It is not a matter of identity. We need to get security. And you think of a door lock or a burglar alarm or a tall wall or a reinforced cockpit door. There are lot of security measures that have nothing to do with privacy.

Chairman LEAHY. Well, but DHS and the other supporters of REAL ID keep saying that we must do all we can to protect ourselves and cost is no object. I would point out the Oklahoma City bomber had a valid driver's license. Nothing would have—if he had been stopped while he was driving that truckload of explosive in a routine check, he had a valid driver's license. The 9/11 hijackers had valid State driver's licenses.

Now, the REAL ID costs, I think DHS is the one that came up with the \$23 billion cost estimate in its draft regulations. They also said they have to update their security standards in 3 to 5 years, adding billions more in administrative costs.

Are we in a "security at any cost" situation?

Mr. SCHNEIER. Clearly we are not. Security is always a tradeoff. Of course, there are always things we can do more. The question is: What has the value?

Chairman LEAHY. Ms. Kephart?

Ms. KEPHART. Well, I have to answer the 9/11 hijacker statement. The 9/11 hijackers had valid driver's licenses and IDs that at least seven of them obtained fraudulently. So the rest of that sentence needs to be there. Also, the REAL ID—

Chairman LEAHY. Well, thank you for telling me what I should say, Ms. Kephart. That is an amazing help, and I cannot thank you enough because I do not have the experience that you have after 32 years here in the Senate dealing with these matters. But let me add to this. They also could have not had to have any kind of an ID like that, and they had a passport. Is that correct?

Ms. KEPHART. They had passports that had much fraud in them as well. That was not detected.

Chairman LEAHY. And that is my point. We have a lot of people who come to this country that have passports, we look at them, and they appear totally valid on their face. You know and I know that both of us could within a matter of hours get passports that could pass scrutiny, and they would be fake passports—the point being if you are going to just rely on what ID you want, you can get fake IDs. Am I correct?

Ms. KEPHART. Absolutely you are correct—

Chairman LEAHY. Could you go to—

Ms. KEPHART.—and REAL ID is set out to address that based on the States' own best practices that they set out in a security document framework in AAMVA. And that is the basis of the REAL ID language.

To answer your original question—

Chairman LEAHY. What in the REAL ID Act is superior to the driver's license provisions in the 2004 Intelligence Reform Act, which was passed after actual negotiation and discussion in a bipartisan way? What is superior in this to the driver's license provisions of the 2004 Intelligence Reform Act?

Ms. KEPHART. It sets out a more detailed set of language that is based on the 13 task force work that was done in AAMVA through the States, and it specifically draws on language that had been done by the States on their own. So it is more specifically geared to what the States wanted to begin with.

Chairman LEAHY. Does it bother you at all that this was passed with absolutely no input, debate, or anything else, just added in?

Ms. KEPHART. Sir, I would have always appreciated that my old Committee that it had gone through, but from what I understand, when Tom Davis drafted this and it went through Mr. Sensenbrenner's Committee, REAL ID was actually put on as a rider to get more votes because at the time it was very popular.

Of course, the Senate should have had a chance to view it—

Chairman LEAHY. Would you—

Ms. KEPHART.—but that is kind of water under the bridge now—

Chairman LEAHY. Do you think this is what—

Ms. KEPHART.—and we are dealing with—

Chairman LEAHY. No, it is not water under the bridge. I mean, you have the Nation's Governors, Republicans and Democrats, who are saying they want to have a voice in this. Should they just be ignored?

Ms. KEPHART. They have a voice—

Chairman LEAHY. Or is this a case—

Ms. KEPHART.—in the proposed rules, sir.

Chairman LEAHY. Is this a case where the Federal Government knows better than the States?

Ms. KEPHART. Absolutely not, which is why—

Chairman LEAHY. Thank you.

Ms. KEPHART.—the comment period has been what it is. Thank you.

Chairman LEAHY. Thank you.

I have other questions concerning what happens if these IDs are lost or stolen, whether they should be an acceptable credential for coming in from Canada. We are now talking about requiring passports to come in from Canada, an interesting thought when you have the largest unguarded frontier in the world. It will actually cut down very substantially the amount of traffic and commerce between two great nations. Any of us who live within a few miles of the U.S.-Canadian border know this will not stop somebody who wants to get across. And if you think it is easy in the eastern part of our country, go out in the western part. As somebody pointed out at one of the border crossings, one in the western part, the security is an orange cone sitting in the middle of the road.

So do we look for substantive changes or do we accept what Ms. Kephart seems to be saying, that we have comment time and basically—and I do not want to put words in your mouth, Ms. Kephart, nor to finish your sentences for you, because I think now how offensive I would find that. But is this a case where we should just let DHS go forward with this? Or should we be seeking legislative changes?

Ms. KEPHART. Sir, I think the appropriate thing to do at this point, because a lot of time, effort, and money has been put into the proposed rules—the comment period ends today—is to see where those comments are. I am sure that the States and many others, including the folks at this table, have issued incredibly helpful comments to DHS. They have taken the privacy aspect of this very seriously. And I think as the comments come in, at the end of that period when it is reviewed and they issue their final rules, I think then is the appropriate time to decide whether to go back to the Intel Reform Act language or to proceed with REAL ID. But I think it is premature at this point, sir.

Chairman LEAHY. Thank you.

Mr. Schneier?

Mr. SCHNEIER. I think that DHS has showed very little respect for the States and the people here. The comments are due today on the draft regulations. DHS has testified that we will get the final regulations by August or September. It is just not possible for DHS to read, review, and consider the thousands of comments they are getting, which tells me they do not intend to make any changes at all.

If I could add one thing about the orange cone, I think the orange cone is a very good analogy to what we are trying to do here. That orange cone works if the Canadian drives right into and fails if he drives around it. And that is what we are doing here with REAL ID. Yes, if the bad guys do the exact thing we want them not to do that the REAL ID will prevent, we will prevent bad things from happening. But it is so easy for the bad guys to drive around it.

Chairman LEAHY. Dr. Carafano?

Mr. CARAFANO. Mr. Chairman, I think there is a bigger problem for the Committee to focus on, and this is, I think, an incredibly

unrealistic requirement in draft legislation for 100 percent electronic verification on everyone in the United States before they get a job. To me, that is truly a national system, unworkable, unachievable, impractical, and that is a much, much bigger drag on our economy and a much, much bigger threat to our privacies and to this country as a whole than REAL ID.

Chairman LEAHY. Mr. Harper?

Mr. HARPER. You have a range of options open to you, of course. Restoring the 9/11 Commission-inspired identity security provisions in the Intelligence Reform and Terrorism Prevention Act is one. I think just as important, part of what you started here, is to have a national discussion on whether identity-based security gets you anything. I think that is most important. It is my opinion that it gets you very little.

There are going to be identification systems going forward, and we should talk about the kinds of systems that can get you maximal security within that area without the surveillance. We are nowhere near that with REAL ID. We are going in the wrong direction. But there are systems we can put together that will solve these problems to the extent they can be solved. Direct security like Bruce Schneier talked about: cockpit doors, tall walls, That is real security. It does not rely on identity, and it does not have any privacy consequences at all.

Chairman LEAHY. Mr. Gilbert?

Mr. GILBERT. If we do anything, I think we should go back to where we were in 2004 when the Intelligence Reform and Terrorism Prevention Act was being discussed. The ACLU and other groups were involved in the rulemaking. There was cooperation. There was discussion among officials on the State level and the Federal level, and then that sort of all got derailed with the REAL ID Act. And now we are sort of 2 years further along, and I think we might be further behind.

But I want to underline what Mr. Harper just said. We in this country have really got to at some point face up to the fact that some things we think are making us safer and more secure might be having the opposite effect, and some things that we could be doing we are simply not doing because we are going for the jazzy things that sound as though they might be making us safer, and I am afraid they are really not. And I really worry that we as a country do not seem to have a level of awareness of the intrusion of electronic data and aggregated data bases in our lives.

Chairman LEAHY. Thank you very much. With that, all of you feel free, if you did not think you had enough time to answer any question, of course, I will provide room in the transcript to note that you wanted to add to that. Or if you find that you wanted to correct something, we will have room for that, and also questions or statements from other Senators. I think this is an extremely important issue. We want to be secure, but we also want our privacy. One of the great things about democracy is that you can usually guarantee both security and privacy. And in this debate it has become almost a cliché, but to make reference to—and I will paraphrase—what Benjamin Franklin said about those who would give up their liberties for some security: You usually end up with neither.

Thank you.

[Whereupon, at 11:46 a.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

Responses to Questions for James Carafano

1. You testified in favor of the REAL ID Act, noting that by providing greater identity security, the REAL ID Act will improve national security.

But REAL ID replaced a law that would have achieved many of the same security improvements, but without an unfunded mandate on the States, and without turning our State DMV officials into immigration officials.

If you believe that the REAL ID Act is a superior security measure to the negotiated rulemaking provisions contained in the 2004 Intelligence Reform Act, please provide me with specific examples as to why.

- I think arguing the two pieces of legislation offer stark alternatives is incorrect. I see them as complimentary. The REAL ID legislation is far superior in establishing minimum document requirements, issuance and processing standards, and requirements for privacy protections. In addition, the IRTP Act of 2004 was overly prescriptive in defining the content of implementing legislation.

2. The draft regulations for the REAL ID Act issued by the DHS do not require that information stored on a REAL ID driver's license be encrypted, which leaves the machine-readable data vulnerable to anyone with the tools to scan the information. Just last week, the DHS' Data Privacy and Integrity Advisory Committee raised serious concerns with REAL ID, calling it "one of the largest identity management undertakings in history," that does not mention any steps states should take to prevent unauthorized access to information on the cards.

Do you have any concerns about the ability of States and the Federal government to manage and secure a database of 260 million people?

- I do have concerns about the ability of states and the federal government to implement the requirements of REAL ID. The answer to these concerns is simple—insist that governments do the job right. Most large-scale information technology programs that fail, fail for the same reasons: inadequate leadership, unclear requirements, unrealistic timelines, and inadequate resources. Rather than trying to gut the requirements of the REAL ID Act, Congress should focus on its appropriation and oversight responsibilities, ensuring the administration has adequate resources to implement the program and a sound management structure to oversee implementation.

Do you have any concerns about the possible creation of a parallel database in the private sector?

- The private sector already maintains data bases with information that has been made available to the public by states and the federal government. REAL ID will not require making any additional information available to the private sector. If states or the federal government wish to restrict public access to data in order to protect individual privacy and such restriction do not conflict with government's obligation to respect Constitutional liberties then they should pass laws restricting public access to this information.

4. Ms. Kephart testified that States are not obligated to comply with REAL ID. But if a State does not comply, then the citizens of that State will not be permitted to enter Federal facilities or board airplanes. This includes, presumably, courthouses, post offices, and any other Federal facility where citizens may in fact be compelled to appear.

Do you believe this is a choice when not complying with the law would arguably result in the forfeiture of a citizen's constitutional rights, such as the right to access a Federal court to petition the government?

- No, REAL ID does not relieve government from its responsibility not to violate the constitutional rights of its citizens.

5. I believe there are troubling parallels between the REAL ID and the Western Hemisphere Travel Initiative (WHTI) programs, as both face serious hurdles to implementation. Some have suggested combining the two documents, or allowing States to issue WHTI-compliant REAL ID cards.

What are your thoughts on making REAL ID compliant licenses an acceptable credentialing document to enter the U.S. from Canada, Mexico, or the Caribbean?

Would it be wise to integrate the WHTI Passcard with the REAL ID Card?

- I see no problem with states that wish to issue driver's licenses that also meet the requirements of WHTI as a convenience to their citizens who want to use state driver's licenses as a border crossing card. I also see no problem with extending reciprocal acceptance to Canadian provinces whose driver's licenses meet standards equivalent to REAL ID and are compliant with WHTI. I don't think it would be prudent at this time to extend reciprocal agreements to other countries in the Western Hemisphere.

**Post-Hearing Questions of Senator Patrick Leahy
“Will REAL ID Actually Make Us Safer?”
An Examination of Privacy and Civil Liberties Concerns”
Senate Judiciary Committee
May 15, 2007**

Questions for Jim Harper:

1. One thing that troubles me about the REAL ID Act is the fact that it was attached as rider on a must-pass appropriations bill, with little debate and without the benefit of hearings. The majority of legislators stripped the REAL ID Act from the 2004 Intelligence Reform bill in favor of a negotiated rulemaking process between the States, stakeholders, and the Federal government, but REAL ID was added back a year later.

What can the American people infer about this law when it was essentially forced on the States outside the normal legislative process?

Response:

The actions of REAL ID’s proponents to gain passage of the law is inductive evidence of its substance. The passage of the law without a hearing, attached to a military spending bill, and without an up-or-down vote in the Senate suggests that it does not add to our nation’s protections.

In our representative democracy, it is normal, expected, and desirable for elected officials to seek credit for their good works. Doing good things in office and getting the word out about such things help to ensure reelection, which is something most Members of Congress and Senators desire.

Fear of terrorists and terrorist attacks is a prominent theme of the national debate since September 11, 2001. This makes security a particularly ripe area for political credit-seeking.

Given these factors — legislators’ self-interest and public concern with potential terrorist attacks — one would expect congressional leaders to promote knowledge of, and seek credit for, a new and effective security proposal. This would typically be done by holding hearings during its consideration, by issuing press releases and holding press conferences, and by having floor votes on the proposal.

But these things did not happen with REAL ID. REAL ID did not receive hearings to tout its effectiveness as a security measure. REAL ID was attached to a military spending bill rather than going through as a free-standing bill. REAL ID wasn’t even mentioned in the President’s signing statement when it became law.

Were REAL ID an effective security measure, and consistent with American values, its proponents would have promoted it relentlessly. And they would have easily (and loudly) defeated opponents of it, because securing the country against terrorist attacks is an agreed-upon national priority.

But they did not promote what they were doing. They did not invite public discussion and debate. They did what they could to force it through Congress with minimum publicity, knowing that it would not survive a full public airing.

Even today, with the Department of Homeland Security “bought into” REAL ID, there has not emerged any advocate that can make a credible case that REAL ID adds to our protections more than it costs in dollars, lost privacy, and lost liberty. As I observed in my written testimony, the DHS’ own study of REAL ID helps to show that it would cost the country more than it would gain us.

There is much pandering to terror fears, and advocates of REAL ID continue to use fear, attempting to buffalo the American people, but this should not cause us to implement REAL ID, which would divert taxpayer dollars from security programs that work.

2. Ms. Kephart testified that the REAL ID Act is not a mandate on the States because States can opt out and inconvenience their citizens with respect to access to Federal facilities and air travel.

Do you agree? Is this a meaningful distinction?

Response:

It’s an entertaining notion, the idea that one can “opt out” of a uniform, government-imposed system at the center of the economy or society, making that system no longer a mandate.

According to that theory, most law is optional. Income taxes are not mandated – they’re just a product of the choice to earn money above a certain threshold. Anyone can “opt out” of that. Environmental laws are the product of the choice to engage in manufacture, transportation, ownership of property, or other productive enterprise. Opt-out is easy. Carrying a driver’s license is the product of a “choice” to exercise autonomy by driving a car. Opt out by staying home.

All practical people recognize that these laws are not optional. Good or bad, they are mandates.

When the Supreme Court ruled in the 1992 case of *New York v. United States* that the federal government could not “commandeer” state governments, federal “mandates” on states in the most technical sense of the term were eliminated as unconstitutional. Yet, three years later in 1995, the new 104th Congress passed the Unfunded Mandates Reform Act. Congress had persisted, despite *New York*, in forcing the states into doing its bidding, often at very high costs. Congress had continued to impose mandates, even without directly ordering states to do things.

Something is mandated when it is commanded directly. It is also mandated when the government conditions a common or essential activity on doing that thing.

But the answer to the question is not all semantics. When the Congressional Budget Office assessed the REAL ID Act in February 2005, its estimate of impacts on state, local, and tribal governments talked about “new mandates with significant additional costs.” Under UMRA, CBO treated REAL ID as a mandate. It’s a mandate.

3. Many Americans – especially older Americans and those who have suffered in the wake of natural disasters – do not have access to important enrolling documents like their birth certificates.

If the DHS agrees that States may waive the requirement for certain “breeder” documents that may have been lost or destroyed, doesn’t this undermine the entire system?

Response:

As I noted in my testimony, the Department of Homeland Security has not articulated how this “system” is intended to secure the country. This makes it very hard to determine what might undermine the system.

The assumption I have made — and on the one I think most people share — is that locking down people’s identity and proof of legal residency would enable DHS to compare people’s proffered identities to lists of known terrorists using government checkpoints at key bottlenecks like airports.

This approach is already riven with flaws, as I noted in my testimony:

- It transfers risk from ID-controlled infrastructure to non-ID-controlled infrastructure;
- It can be avoided through the recruitment of accomplices without records of crime or terrorism; and

- It can be defeated through the acquisition of false documents by forgery or bribery.

Allowing people without breeder documents to acquire REAL ID compliant licenses and IDs widens the forgery and bribery holes in the REAL ID “system.” It would be easier to dupe a DMV employee into issuing a license and it would be easier to pay off a DMV employee to do so with this waiver. Undermining the REAL ID “system” in this way would be somewhat analogous to drilling an additional hole in swiss cheese.

4. I believe there are troubling parallels between the REAL ID and the Western Hemisphere Travel Initiative (WHTI) programs, as both face serious hurdles to implementation. Some have suggested combining the two documents, or allowing States to issue WHTI-compliant REAL ID cards.

What are your thoughts on making REAL ID compliant licenses an acceptable credentialing document to enter the U.S. from Canada, Mexico, or the Caribbean?

Would it be wise to integrate the WHTI Passcard with the REAL ID Card?

Response:

The similarities between REAL ID and WHTI do not end at implementation hurdles. The more fundamental similarity is that both programs carry more costs than they provide increased security to the country.

WHTI is already doing a great deal to increase the costs and, accordingly, reduce the frequency and robustness of cross-border trade and travel. This daily saps the vitality of the U.S. economy and the economies of other countries in the region, rendering our societies weaker and reducing employment, wealth, and health.

Like REAL ID, the security benefits of WHTI are insignificant. There are a variety of ways to avoid WHTI, or to access the country with evil intent despite WHTI. Combining these two failed security systems, or making them interoperable, is no solution. Neither REAL ID nor WHTI should be implemented.

**Post-Hearing Questions of Senator Patrick Leahy
 “Will REAL ID Actually Make Us Safer?”
 An Examination of Privacy and Civil Liberties Concerns”
 Senate Judiciary Committee
 May 15, 2007**

Questions for Janice Kephart

1. Ms. Kephart, you testified in favor of the REAL ID Act, noting that by providing greater identity security, the REAL ID Act will improve national security.

But REAL ID in fact replaced a law that would have achieved many of the same security improvements, but without an unfunded mandate on the States, and without turning our State DMV officials into immigration officials. I asked you during the hearing why you believed that the REAL ID Act was superior to the negotiated rulemaking provisions contained in the 2004 Intelligence Reform bill, and in reviewing your response, you provided no specific reasons as to why you believe the REAL ID Act is superior. Your response to this question during the hearing was as follows:

It sets out a more detailed set of language that is based on the 13 task force work that was done in AAMVA through the States, and it specifically draws on language that had been done by the States on their own. So it is more specifically geared to what the States wanted to begin with. (Tr. at page 68).

Please provide me with specific examples as to why you believe the REAL ID Act is superior to the negotiated rulemaking process, which was passed as part of the 2004 Intelligence Reform Act.

ANSWER. I will take the answer in five parts, four of which involve the premise of your question.

1. *REAL ID in fact replaced a law that would have achieved many of the same security improvements.*

Answer. Real ID contains extensive language for the purpose of setting out minimum standards *of security* all states should meet to assure a foundation for ID issuance security across all states. What REAL ID did was improve Section 7212 of the Intelligence Reform and Terrorism Prevention Act of 2000 (IRTPA), for the reasons I set out in the answer to the question during the hearing.

2. *REAL ID in fact replaced a law that would have achieved many of the same security improvements, but without an unfunded mandate on the States.*

Answer. The IRTPA did not provide any specific funding to the States to develop minimum standards for driver's licenses; the premise in the question is incorrect.

3. *REAL ID in fact replaced a law that would have achieved many of the same security improvements, but without an unfunded mandate on the States, and without turning our State DMV officials into immigration officials.*

I do not read the Notice of Proposed Rulemaking (NPRM) as turning State DMV officials into immigration officials. What the law and the NPRM require is that an individual must prove their legal status in the U.S. before obtaining a Real ID compliant license or ID. The NPRM did not require DMV officials to take any particular action when a person could not establish their lawful status in the U.S. except refusing to issue that individual a Real ID compliant document. That action does not turn a DMV worker into an immigration official. And in fact, all the DMV official will likely have to do under the minimum standards—although they are not final yet—is to check two separate federal databases—SAVE and the passport database—for a determination as to eligibility. Of course, a State may decide to impose more checks re lawful status, which a State is entitled to do under the law, but that is certainly not required.

Simply refusing to confer a benefit to which a person is not legally entitled does not somehow transforms DMV workers into immigration officials, the same as refusing an underage driver a license turns a DMV worker into a juvenile carctaker.

4. *I asked you during the hearing why you believed that the REAL ID Act was superior to the negotiated rulemaking provisions contained in the 2004 Intelligence Reform bill, and in reviewing your response, you provided no specific reasons as to why you believe the REAL ID Act is superior.*

Answer. Upon review of the transcript sent to me for review by your Committee, on p. 68 Senator Leahy posed this question to me: “What in the REAL ID Act is superior to the driver’s license provisions in the 2004 Intelligence Reform Act, which was passed after actual negotiation and discussion in a bipartisan way? What is superior in this to the driver’s license provision?”

As you can see, there was no mention in that question of negotiated rulemaking. The statement ‘actual negotiation and discussion in a bipartisan way’ referred, in the context of our conversation, to the process of the law passing, not the substance of the law itself.

And thus I answered the question asked of me—what was superior about REAL ID over the Intel Reform Act?—as follows:

“It sets out a more detailed set of language that is based on the 13 task force(s) work that was done at AAMVA through the States, and it specifically draws on language that had been done by the States on their own. So it is more specifically geared to what the States wanted to begin with.”

We continued our dialogue on that point but ‘negotiated rulemaking’ was never brought up by the Senator.

5. Please provide me with specific examples as to why you believe the REAL ID Act is superior to the negotiated rulemaking process, which was passed as part of the 2004 Intelligence Reform Act.

Answer. I never said that a negotiated rulemaking process was inferior or better than the REAL ID Act. Thus, your premise is incorrect. What I said and will continue to say is that other provisions of REAL ID are stronger than the 2004 IRTPA, and thus, since REAL ID fulfills the 9/11 Commission recommendations on secure IDs alongside of AAMVA's prior work on secure IDs, it is on the whole a better law. Moreover, since the NPRM are not only out but closed for comment, and ALL parties, not just parties that were invited to the table for negotiated rulemaking (which were limited) have now had ample opportunity to weigh in to DHS on behalf of the final rule, I will repeat what I did at the hearing, which is that the Committee wait and see until the Final Rule comes out this fall to make a determination as to whether or not the law the REAL ID Act NPRM process was a better process than negotiated rulemaking, or whether it should be revamped.

2. The draft regulations for the REAL ID Act issued by the DHS do not require that information stored on a REAL ID driver's license be encrypted, which leaves the machine-readable data vulnerable to anyone with the tools to scan the information. Just last week, the DHS' Data Privacy and Integrity Advisory Committee raised serious concerns with REAL ID, calling it "one of the largest identity management undertakings in history," that does not mention any steps states should take to prevent unauthorized access to information on the cards.

Do you have any concerns about the ability of States and the Federal government to manage and secure a database of 260 million people?

Answer. DHS is the appropriate entity to answer the technical issues raised by the introduction to your question.

As to the question you ask, Congress did not recommend that REAL ID be one database or a national database. While protecting privacy and state prerogatives, the law envisions a partnership among the states and the federal government. The NPRM states that the information collection and data verification network to implement REAL ID would remain a state controlled and operated business process and one that the federal government would not participate in. It is my belief that it is the responsibility of every level of government to protect its citizens; that is why the 9/11 Commissioners wrote the secure IDs recommendations in *The 9/11 Final Report* in the manner they did.

More specifically, my understanding is that there will not be any database of 260 million people. The only databases that are brand new and created for the purpose of fulfilling REAL ID requirements are the digitized birth and death records--vital events records—under Section 7211 of the Intelligence Reform Act. (See p. 17 of my paper *Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security* for more information on this point, located on my website 911securitysolutions.com.) The vital events or EVVE database, like all the state databases under REAL ID—Commercial Driver License Information System & National Driver

Register and EVVE—will be only held by the states that originate the information and sharing of information will be limited, on an as needed basis, and in limited fields of information.

The only information the federal government will hold under REAL ID will be information it already holds and, for the most part, already shares with the states prior to REAL ID implementation. This includes SSOLV (SSNs), SAVE (lawful presence), and DOS passports (exists but needs a means to network to states). The vehicle for sharing the information is the privately own network of the DMVs—AAMVA-- so even here you do not have a federal breach into acquiring more information on persons than already exists.

Do you have any concerns about the possible creation of a parallel database in the private sector?

Answer. No. I have no knowledge of the possible creation of any ‘parallel’ database, nor could there be one, as different types of data is stored separately, as described above. In addition, the private sector has no access to such information. The 1994 Driver’s Privacy Protection Act bars State employees from selling or releasing personal information such as Social Security numbers, photographs, addresses, phone numbers and birth dates of applicants. The law has been upheld by the Supreme Court and must be incorporated into REAL ID implementation.

3. You testified that States are not obligated to comply with REAL ID. But if a State does not comply, then the citizens of that State will not be permitted to enter Federal facilities or board airplanes. This includes, presumably, courthouses, post offices, and any other Federal facility where citizens may in fact be compelled to appear.

Do you truly believe this is a choice when not complying with the law arguably results in the forfeiture of a citizen’s constitutional rights, such as the right to access a Federal court to petition the government?

Answer. As long as there is another means for a citizen to enter a federal courthouse, by producing a different combination of IDs that is acceptable under the REAL ID regulations—a question that DHS can answer better than I—I do not see any forfeiture of rights. I see a balance between an individual’s right to petition his government and the nation’s right to reasonably secure against individuals that may seek to conduct harm.

By way of background, however, what DHS has repeatedly stated on this point in town hall meetings they have held with DMVs and other interested parties in the last couple of months is as follows: A non-complying state driver’s license or ID could not be used for access to those facilities that require a REAL ID driver’s license to gain access. Other acceptable forms of identification documentation such as a passport or military card will still be accepted in lieu of a REAL ID driver’s license or identification card to gain access to federal facilities such as those noted above.

4. You testified that many States have been taking the initiative to improve the security of their driver’s licenses without being mandated to do so by the Federal government.

If this is so, why do you believe we need the Federal Government mandating a process that in many places, according to your testimony, is already underway?

Answer. Many states are in the process of or already have invested in IT, infrastructure and security upgrades in their ID issuance regimes that will likely be REAL ID compliant. Not every state is at the same stage, of course, due to legal, budgetary, staffing and political issues either paving or blocking the way towards improved security.

Requiring minimum set standards is a very good idea—in fact this was the idea of the states to begin with when they set up the Secure Document Task Forces in AAMVA after 9/11—to assure that all States can meet minimum standards. Infusing integrity into a State ID issuance systems that the States themselves acknowledged as broken after 9/11; after it was obvious how easily the 9/11 hijackers defrauded the system; how easily it still is to defraud ID issuance systems in many states today, is an imperative for security. Not doing so simply keeps our nation vulnerable.

Wouldn't it be more desirable to have a process in which the States are not only assisted financially by the Federal government, but also have a seat at the table? It seems to me a process like this would help gain the buy-in necessary for success from all those affected.

Answer. This is an excellent point; the States should be financially supported in coming into compliance with REAL ID.

The States do have a seat at the table; all interested parties to REAL ID have had an opportunity to buy-in during informal negotiations prior to the proposed rules being published March 1, 2007 and most certainly during the comment period for the proposed rules, which closed the date of your hearing, May 8, 2007. In fact, the comment period opens buy-in to everyone, instead of just a few selected interested parties under the IRTPA you refer to in your first question. The States themselves have been involved to the extent they have sought involvement alongside their associational representation via NCSL, AAMVA and the NGA. Groups like the ACLU have also submitted extensive comments. In my view, it is actually a better system to achieve buy-in from all interested parties rather than just a few select associations or groups that may not be fully representative of all interested parties in the public and private sector.

5. In the biography you provided to the Judiciary Committee, you stated that you “continue[] to work with the Canadian Embassy . . . in an effort to pursue the implementation of recommendations sought by both the 9/11 Commission and borne of her own work.”

Please describe in detail the work you have done, or continue to do with officials at the Canadian Embassy, and the names and positions of the Embassy officials with whom you have worked.

Answer. I have worked with the Congressional liaison, political, economic and border personnel at the Embassy in regard to the Western Hemisphere Travel Initiative. I will continue to be available to them as necessary; continue to be invited to Embassy functions; and have organized

policy panels where such personnel have participated, including their most senior Washington staff.

6. I believe there are troubling parallels between the REAL ID and the Western Hemisphere Travel Initiative (WHTI) programs, as both face serious hurdles to implementation. Some have suggested combining the two documents, or allowing States to issue WHTI-compliant REAL ID cards.

What are your thoughts on making REAL ID compliant licenses an acceptable credentialing document to enter the U.S. from Canada, Mexico, or the Caribbean?

Would it be wise to integrate the WHTI Passcard with the REAL ID Card?

Answer. Although they appear to be parallel there are significant differences between the WHTI Passcard and a REAL ID. A WHTI compliant document indicates a person's citizenship at a federal level, the REAL ID Act does not require this information and is still a card issued by a State that, unless the State chooses to do so, does not indicate citizenship. In fact, REAL ID specifically permits non-citizens lawfully present in the U.S. to obtain a REAL ID compliant driver's license or ID. A REAL ID compliant license would not by itself satisfy the critical WHTI requirements.

Moreover, whether a driver's license is REAL ID compliant or not, unless a border inspector is given the tools to determine:

1. whether that REAL ID driver license is fake or not;
2. knows all States denote citizenship and does not have to differentiate between them in 45 seconds or less to conduct an inspection;
3. the cards can be subject to watchlist and other federal checks as are passports;

this nation is a long way from having REAL ID driver licenses as the acceptable means of entry across our borders.

The same answer goes for combining the two cards. However, I am more than willing to wait and see the results of the Washington State pilot and the (potential) Michigan State pilot before I come to a firm conclusion.

Thank you for your questions and your interest.

Sincerely, Janice Kephart

**Post-Hearing Questions of Senator Patrick Leahy
“Will REAL ID Actually Make Us Safer?”
An Examination of Privacy and Civil Liberties Concerns”
Senate Judiciary Committee
May 15, 2007**

Questions for Bruce Schneier:

1. At the Judiciary Committee’s hearing, you testified about the relative ineffectiveness of identity-based security systems.

Assuming that identity-based security has some place in the larger national security picture, what suggestions would you give the Committee in terms of identity-based security measures that can be effective?

Identity-based security is valuable as an access control device. For example, airports use identity based security to verify mechanics and other airport workers. Businesses use identity-based security to verify who is allowed in the buildings and on the computers. I think a more robust identity-based system makes a lot of sense in these, and similar, applications. It’s when the system is applied to the population as a whole that it fails as a security measure.

2. The draft regulations for the REAL ID Act issued by the DHS do not require that information stored on a REAL ID driver’s license be encrypted, which leaves the machine-readable data vulnerable to anyone with the tools to scan the information. Just last week, the DHS’ Data Privacy and Integrity Advisory Committee raised serious concerns with REAL ID, calling it “one of the largest identity management undertakings in history,” that does not mention any steps states should take to prevent unauthorized access to information on the cards.

Do you have any concerns about the ability of states and the federal government to manage and secure a database of 260 million people?

It would be impossible to secure a database of this size. The DHS has maintained that the problem is easier because it is not one single database, but 50-plus individual databases that are connected. But that’s a semantic dodge; they’re the same thing. The REAL ID database is a single database, regardless of how it is technically configured and organized.

Securing a database of that size is very difficult, as the daily litany of personal-information exposures demonstrates. The REAL-ID database will be particularly difficult to secure because of several reasons other than its size.

One, it will be accessible by law enforcement officers – and potentially at airport security checkpoints and other locations – in all jurisdictions all over the country by tens of thousands of people. This means that it is more likely that someone will give away his password or otherwise allow outsiders to view the information. This also means that it is more likely that trusted law enforcement officers will access the data for personal use.

Two, it will contain highly valuable information, and hence be an attractive target to criminals. As a single point of personal information, the REAL ID database will likely receive more hacking attempts than smaller databases with more limited uses.

And three, it will be cobbled together from 50-plus individual databases. This means that a vulnerability in one state's database will put everyone at risk.

Do you have any concerns about the possible creation of a parallel database in the private sector?

There is a robust data broker industry in the U.S. that maintains databases filled with personal information about every one of us. Already this industry collects information from driver's licenses, either by purchasing that information from the states or from organizations that collect it individually. I have had my driver's license photocopied when I checked into hotels, and I have had my license scanned when entering bars. This information is regularly sold to data brokers, who collect and resell it to others.

Google for "drivers license scanner," and you too can buy a small device that reads the information off all U.S. driver's licenses.

There is absolutely no reason to believe that this practice will cease if licenses become REAL ID compliant. Data brokers will create parallel databases that contain the same information that is on a REAL ID license.

3. Many Americans – especially older Americans and those who have suffered in the wake of natural disasters – do not have access to important enrollment documents like their birth certificates.

If the DHS agrees that States may waive the requirement for certain "breeder" documents that may have been lost or destroyed, doesn't this undermine the entire system?

Yes. Any identification system is only as good as the enrollment procedures. That is, REAL ID can be no more secure than the breeder documents required to get one. And if the system waives the requirement for such breeder documents, it can't provide the identification verification it claims to.

Is there a viable alternative to addressing the likely reality that some applicants simply will not have access to the required documents should the REAL ID Act come into effect?

Unfortunately, there isn't. If someone doesn't have the documents required to get a REAL ID, either because those documents have been lost or destroyed, or because they never existed, the system can either refuse him a REAL ID or give him a REAL ID anyway. And if REAL ID becomes a requirement to receive government services, this will turn into a real barrier – especially in poor rural communities where the documents are hardest to get.

4. I believe there are troubling parallels between the REAL ID and the Western Hemisphere Travel Initiative (WHTI) programs, as both face serious hurdles to implementation. Some have suggested combining the two documents, or allowing States to issue WHTI-compliant REAL ID cards.

What are your thoughts on making REAL ID compliant licenses an acceptable credentialing document to enter the U.S. from Canada, Mexico, or the Caribbean?

I see nothing wrong with the old system of allowing conventional driver's licenses as acceptable documents to enter the U.S. from Canada, Mexico, or the Caribbean. Allowing a REAL-ID-compliant license is certainly no worse than that. And forcing residents of the U.S. and those other countries to get yet another identity document is a serious burden.

Would it be wise to integrate the WHTI Passcard with the REAL ID Card?

At this point, yes. In general, we are more secure with a distributed identity system: a variety of ID cards and credentials, each for its own purpose. But in this case there is no additional insecurity in allowing driver's licenses – REAL ID compliant or otherwise – to be used as identity documents for the WHTI program.

SUBMISSIONS FOR THE RECORD

American Association of Motor Vehicle Administrators

**Statement of Michael R. Calvin, Interim President & CEO
American Association of Motor Vehicle Administrators**

**Senate Committee on Judiciary
"Will REAL ID Actually Make Us Safer? An Examination of Privacy
and Civil Liberties Concerns"**

May 8, 2007

Thank you for providing the American Association of Motor Vehicle Administrators (AAMVA) the opportunity to provide a written statement for the printed record to discuss the impact of The REAL ID Act (P.L. 109-13) on privacy, the ability of motor vehicle agencies to protect personal information, the use of the Commercial Driver's License Information System (CDLIS) to serve as the platform for an all-driver system and who should have access to motor vehicle agencies data.

AAMVA is a state-based, non-profit association representing motor vehicle agency administrators and senior law enforcement officials in the United States and Canada. Our members are the recognized experts who administer the laws governing motor vehicle operations, driver credentialing, and highway safety enforcement.

As you know, comments are due today for the REAL ID Notice of Proposed Rulemaking (NPRM) to the Department of Homeland Security (DHS). DHS requested comments on several aspects of privacy from encryption to best practices for protecting the privacy of personal information. AAMVA members recognize the importance of privacy and confidentiality of information and the protection of customer information in all forms of use, access and dissemination.

**PRIVACY AND PROTECTION OF PERSONAL DATA FOR THE DOCUMENT
VERIFICATION SYSTEMS AND STATE-TO-STATE INFORMATION EXCHANGE
SYSTEMS STIPULATED IN THE PROPOSED REGULATIONS**

AAMVA members recognize that Congress and DHS are very interested in the governance of the verification systems and interoperability of systems to achieve the requirements of the REAL ID Act. AAMVA members are very interested in helping to determine the governance structure of any systems that potentially could interface with state driver licensing systems and federal verification systems. AAMVA members recognize the importance of system access, use and control. They also recognize the importance of security, and protecting the privacy of personal information. This is also of paramount concern to their governors and state legislators. In order to ensure that careful consideration is given to all the components of governance and exactly

what systems will be governed, AAMVA members formed a working group which is currently working on a proposal for DHS. It is not yet completed. AAMVA will file supplemental comments to the NPRM with governance recommendations once the governance working group has completed its work. Those supplemental comments will also include a recommended prioritization of the required verification systems and document verification systems options based on risk and value.

AAMVA members want to emphasize that governance of DMV related systems and any accompanying verification systems are critical to the states. While the structure for governance has yet to be recommended to Congress and DHS, it is imperative to note that states expect to have control over their systems, the information which is their responsibility, and the processes that govern any use or access. AAMVA members will remain acutely interested and active in a continued dialogue regarding system governance, system prioritization and data privacy.

Many states have privacy laws that are more restrictive than the Drivers Privacy Protection Act (DPPA). AAMVA members will continue to work with DHS on ensuring privacy, and are more than willing and prepared to provide specifics on privacy protection in their security plans provided to DHS. AAMVA members remain very interested in the “federal reference” databases and will continue to provide input to DHS on the development, governance and protection of the data and information in those databases. DHS has yet to provide specific information on how this “query” system will work and does not expect to provide that information until the comment period is over.

AAMVA members are more than willing to work directly with Congress and DHS on these systems and privacy issues and implications. The Governance Working Group in developing its proposal is using privacy principles contained in AAMVA’s *Driver’s License/Identification Card Security Framework*, as the basis for protecting privacy and motor vehicle agency data. The working group and AAMVA and its members recognize the importance of privacy and put forth the following eight Privacy Principles to underpin the governance structure:

1. Openness: Each DMV shall inform the public of all systems and databases that are being established or have been established for use in driver’s license and identification card issuance; the public shall be informed of the nature of the information systems that are maintained and used for the purposes of administration of the laws that pertain to the licensing of drivers.
2. Individual participation: Each individual has the right to examine the data kept on himself/herself by the DMV and request the making of corrections to that data.
3. Collection limitation: Each DMV shall have a clear list of required personal data elements.
4. Data quality: Each DMV shall ensure that all data is “accurate, complete, current and verified.”
5. Use limitation: Each DMV shall specify how it uses personal information and shall adhere to this specification.

6. Disclosure limitation: Each DMV shall adhere to a specified disclosure limitation that indicates what personal information may be disclosed and how it may be disclosed.
7. Security: Each DMV should protect all data kept.
8. Accountability: Each DMV shall ensure it has a means to oversee and enforce the previously mentioned principles.

As proposed in the NPRM, each state is required to submit, as part of The REAL ID Act certification process, a written comprehensive, security plan. States are prepared to address privacy in their comprehensive security plans and, in fact, many states already have these types of plans and procedures in place. Privacy and confidentiality concerns are not a new issue to state DMVs, nor are their application. AAMVA members also recommended to the agency that DHS continue to emphasize AAMVA's member-developed model legislation to prohibit the capture and storage of personal information obtained from a driver's license or identification card--as DHS' Privacy Office has referenced in the Privacy Impact Assessment published with the NPRM. We also recommend that Congress work with DHS and the states to strengthen the Drivers Privacy Protection Act.

DOCUMENTS VERIFICATION SYSTEMS

AAMVA members support the need to electronically verify documents that are presented for driver's license and identification card issuance based on the value that the verification provides. Many of the issues surrounding driver's license fraud and abuse are the result of counterfeit or fraudulent breeder documents. In its *Driver's License/Identification Card Security Framework*, AAMVA points out that wherever possible, all jurisdictions shall electronically verify the identity documents presented by applicants to prove identity, required for driver's license or identification card issuance, with the originator of those source documents. Almost all jurisdictions now use the Social Security On-Line Verification system. AAMVA members are interested in getting additional support from the federal government in the remaining required electronic verification systems as some are critical to the DMV business. However, the entire verification area is vexing and the NPRM is concerning on a number of levels. Time and money top the list along with system development and deployment.

1. Privacy and security of any personal information is paramount and must be an overriding guiding principle in any system development and use.
2. Any verification system development must minimize the effect on state DMV processes and must be integrated into the AAMVAnet infrastructure--an infrastructure that states use now for connectivity to existing verification programs and requirements such as SSOLV, CDLIS, PDPS and the National Motor Vehicle Title Information System (NMVTIS). AAMVA members emphasize that states do not now and cannot in the future use verification systems that require the input of different names on different documents for individual system queries. This would result in significant front line service issues,

employee training issues and computer system issues. The integration into a “one-call” system through AAMVAnet is critical.

3. AAMVA members understand DHS’ use of the term “federated” not to include any wholesale database or data access and also understand that the term relates to an information technology structure that would provide “portal” access for states similar to what states now use with AAMVAnet to access SSOLV, CDLIS, PDPS and NMVTIS.
4. AAMVA members assert that any cost or development of any system be borne by the federal government to meet this federal requirement.
5. DHS should focus on verification systems that have the highest impact and the best value for DMVs to address abuse and fraud in the driver licensing and identification card issuance systems. Currently, high value verification tools exist that can and do reduce the likelihood of fraud--tools that many states are using in the data verification, document authentication and identity assurance areas. Tools such as social security number verification through SSOLV, immigration status verification through SAVE, document authentication through machine verification, document authentication through inspection and photo matching verification are all in use today in many DMVs and are yielding results. DHS should provide the flexibility to states to continue to use these types of tools to meet compliance and certification for REAL ID and should recognize that this direction is an area that yields high fraud detection and reduction results.
6. AAMVA members recommend that DHS view the implementation of verification systems required under the Act through a phased and flexible approach recognizing that some systems like SSOLV and SAVE and tools such as AAMVA’s Digital Image Exchange have the highest value and risk mitigation. DHS should also recognize that proposed verification systems such as the passport verification system have little risk mitigation value and that there are other ways to achieve any value that may be obtained by a full scale and costly birth certificate verification system. AAMVA members assert that there are ways to achieve the mitigation of the fraudulent use of documents through various alternative verification and authentication channels aside from the immediate development of all the five verification systems required in the NPRM.
7. Re-enrollment verification must be left up to states based upon their own individual processes, computer system capabilities and issuance systems as well as their own knowledge of risk mitigation and fraud prevention and detection. As noted in other areas of this response to the NPRM, customers should be “grandfathered in” and re-enrolled automatically if they have been licensed or have had an identification card for 10 consecutive years in a state, if their social security numbers have been verified in SSOLV and their image has been verified. The Final Rule needs to be flexible enough to allow states to be able to make re-enrollment decisions that meet their particular circumstances.

Recent discussions with DHS reveal that a willingness does exist to work closely with AAMVA members on the prioritization, value and use of the verification systems and a willingness to

understand the constraints, challenges and tools that states are currently using to verify documents and combat fraud.

AAMVA has established a number of working groups of members to assess all of the verification systems required and urges DHS to continue to work with AAMVA's members on determining the requirements of these systems.

INTEROPERABILITY

Section 202(d) (6) of the REAL ID Act of 2005 specifies that a state has to: "Refuse to issue a driver's license or identification card to a person holding a driver's license issued by another state without confirmation that the person is terminating or has terminated the driver's license". This provision is similar to that of the Commercial Motor Vehicle Safety Act (CMVSA) of 1986 that required commercial drivers to have one and only one commercial driver license at any given time. This requirement known as the one driver/one record/one license concept is currently supported by CDLIS.

States have been working toward driver licensing interoperability for many years. The partnership AAMVA and its members have with the US DOT has helped advance interoperability for commercial driver licensing through the CDLIS and has conceptually advanced an all-driver system known as DRIVERs (the Driver Record Information Verification System). These concepts are fundamental to highway safety and the *Driver License Agreement* interstate compact among states.

CDLIS has operated in all 51 U.S. jurisdictions (50 states and the District of Columbia) since April 1, 1992. As of March 16, 2007, CDLIS has 13.2 million records, growing at an average rate of more than 40,000 new records per month. CDLIS consists of a Central Site and nodes at the Motor Vehicle Agencies (MVAs) of the 51 jurisdictions. The Central Site houses identification data about each commercial driver registered in the jurisdictions, such as:

- name
- date of birth
- Social Security Number
- state driver license number
- AKA information
- sex
- height
- Current "State of Record" (SOR)

This information constitutes a driver's unique CDLIS Master Pointer Record (MPR). Each MVA houses detailed information about each driver for which it is the SOR. This detailed information, called the driver history, includes identification information, license information, and a history of convictions and withdrawals, and remains in each individual jurisdiction—not in a central data base.

When a jurisdiction MVA queries CDLIS to obtain information about an applicant prior to issuing a CDL, the CDLIS Central Site compares data provided by the State Of Inquiry (SOI) against all MPRs in CDLIS. If one or more matches are returned, then the CDLIS Central Site

"points" the inquiring jurisdiction to the jurisdictions where those matches have been found. The SOR can then provide the detailed information about the driver's commercial driving history.

In accordance with the CMVSA of 1986, access to CDLIS is authorized to only the state driver's license agencies, the Federal Motor Carrier Safety Administration (FMCSA), employer or prospective employer of a person who operates a commercial motor vehicle and federal agencies upon written request and approval by FMCSA where there is a legal basis and need to access the information commercial motor vehicle drivers who wish to review and, if necessary correct information about them in CDLIS. The Commercial Driver License Program, with CDLIS as its primary tool, has significantly reduced fraud in the commercial driving environment over the past 15 years. And AAMVA is not aware of any privacy breaches of CDLIS since it first went in production in 1989. Access to CDLIS is provided via a secure private network operated by the American Association of Motor Vehicle Administration and cannot be accessed via the Public Internet. Each site connected to the private network has its access controlled via several security mechanisms which include:

- a network security layer which restricts each site's network access to its authorized trading partners.
- a messaging infrastructure which also restricts the network traffic to only the authorized locations, and
- finally a security table at the CDLIS central site level controlling access levels on a site by site basis.

On August 10, 2005, Congress passed the transportation reauthorization bill, the "Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users" (SAFETEA-LU), and authorized \$28 million to modernize CDLIS. This effort is currently underway and is scheduled for completion by the end of 2010. While modernization of CDLIS will incorporate recommendations from the CDL Advisory Group, which is comprised of industry, state officials and stakeholder organizations, an enhance CDLIS pointer file could look different from what we know today based on the latest technology. AAMVA and its members are recommending leveraging this project and the federal funding associated with it to expand the scope of the CDLIS modernization effort to support an all-driver pointer system for non-commercial driver's licenses and ID cards. Using the proven CDLIS architecture, this system will provide the jurisdictions with a robust driver license/ID card pointer system, designed to handle 250 million records. This system will allow the jurisdictions to enforce the concept of one person/one REAL ID document/one record mandated by the REAL ID Act.

The use of a CDLIS like system to support the REAL ID requirements will not increase the risk of data privacy breaches.¹ In fact, when Congress passed the Motor Carrier Safety Improvement Act (MCSIA) of 1999 (Pub. L. 106-159, 113 Stat. 1759), it required that all drivers, both commercial and non-commercial, be checked through CDLIS before motor vehicle agencies issue or renew a driver's license. The thought is that if the person is allowed to have more than one license, they will spread their traffic violations across those licenses and therefore avoid driver control action and pose a highway safety risk. As noted in the DHS *Privacy Impact Assessment*, issued in conjunction with the REAL ID Notice of Proposed Rulemaking:

¹ DHS Privacy Impact Assessment REAL ID Act Proposed Rule March 1, 2007, Page 11

As described in Section II.E of the NPRM, although the REAL ID Act poses a requirement for this state-to-state data exchange, this exchange is already required and implemented under the Department of Transportation's (DOT) existing rules and regulations governing commercial driver's licenses (CDLs). The DOT requires that states connect to the National Driver Register (NDR)/Problem Driver Pointer System (PDPS) and the Commercial Driver's License Information System (CDLIS) in order to exchange information about commercial motor vehicle drivers, traffic convictions, and disqualifications. A state must use both the NDR/PDPS and CDLIS to check a driver's record, and also check CDLIS to make certain that the applicant does not already have a CDL. Under these programs, as well as under the REAL ID Act, the primary purpose of the state-to-state data exchange is to determine if the applicant is unqualified and if the application is fraudulent rather than specifically verifying the applicant's identity.

The existing state-to-state data exchange among DMVs, while focused on commercial driver's licensing, also impacts non-commercial license applicants, as states are required currently to run all license applicants against the PDPS and CDLIS, which are both pointer systems that collect limited information from each state in order to match against the incoming inquiries. Both systems offer certain mandatory privacy protections.²

The states are very familiar with the CDLIS program and the all-driver pointer system would use the same principles as CDLIS; however, the technology used will allow for increased security and privacy protection.

Until an all-driver system is fully developed, operational in real time and accessible to all states (with funding provided by the federal government) the concept of ensuring that a person does not have another license or identification card in any other jurisdiction is impossible, and this interoperability requirement is moot. It is possible for states to verify with the prior state or states of record completing a "state to state" check (and many do), but an all national check and the systems to support those checks are far from a reality. It will take considerable effort and funds to get there. Until a national all-driver system is federally funded and available, AAMVA members have recommended that states continue to use CDLIS to query if a commercial drivers license exists. They do this now for all commercial and non-commercial drivers as required by the Motor Carrier Safety Improvement Act (MCSIA). States can also require applicants to self-declare the existence of prior licenses and identification cards and require their confiscation and notification to cancel to the prior state upon the issuance of a new document. Many states also do this presently.

Other AAMVA member recommendations for an all-driver system are:

- access to state information is defined as query and response, not wholesale penetration;
- any access must adhere to the DPPA and more restrictive state record confidentiality laws; and,

² DHS Privacy Impact Assessment REAL ID Act Proposed Rule March 1, 2007, Page 10-11

- access and use are limited to driver's license and identification card issuance and law enforcement management.

It is AAMVA members' recommendation that when a licensed driver or identification card holder moves to a new state, the record will be transferred to the new state. Minimum information will be retained by the former state based on its laws and practices and in accordance with the DPPA. This is the ideal system. But, AAMVA members remain interested in working with DHS to develop alternate solutions to ensuring one driver, one record for all driver's licenses and identification cards.

As stated in the Notice of Proposed Rulemaking, DHS is working closely with the DOT, AAMVA, and the states to fulfill the requirements for the state-to-state data exchange while also supporting privacy protections for this exchange. DHS in consultation with the Department of Transportation still has not yet determined whether CDLIS or some other service will be the platform for the state-to-state exchange. However, whatever platform is chosen, it will be necessary for the states, working with DHS and DOT, to define the privacy protections for any state-to-state data exchange, including how it will be operated and controlled and who will have access.

Machine readable technology on the driver's license or identification card

Many of the provisions in the NPRM concerning machine readable technology on the driver's license and identification cards basically follow the Machine Readable Technology (MRT) requirements of the AAMVA *Driver Licensing/Identification Card Design Specification*. Most states are currently using or moving toward the PDF417 standard as contracts come up for renewal or re-bid. AAMVA members are supportive of all the requirements noted in the NPRM for the machine readable portion of the REAL ID compliant driver's license or identification card, with the exception of the mandatory requirements of full name history and name changes. These should be optional elements for states. AAMVA members recommend that the only mandatory minimum requirements for the MRT be those noted in the AAMVA *Driver Licensing/Identification Card Design Specification*.

Encryption is an area where AAMVA members, and especially its law enforcement members, have concerns. The information/data carried in the common MRZ is the same information/data that is human-readable on the driver's license or identification card. There are a number of good reasons for leaving it this way. A principal argument against encryption is the automation benefit that having access to the information has afforded DMVs and law enforcement in their line of duty. Being able to access the information/data is critical to current and future projects that provide interoperability within this community. Whether it is a customer visiting their local DMV office or a police officer completing a citation/report, that process is greatly enhanced by allowing for the information/data to be read and verified. Were there to be a problem with having access to the decryption key, if the information/data on the credential was encrypted, then obviously this would have a tremendous impact on those processes. There too are economic challenges of rolling out an encryption methodology and infrastructure that go well beyond the REAL ID Act. Key management is a huge concern. There would be the ongoing cost and administration of distributing and protecting the key(s) used for encryption/decryption. The

encryption key(s) would eventually be compromised and released to the general public, rendering them useless. Changing keys would be costly and would not protect existing encrypted credentials.

Attention needs to be focused on the misuse of the information on the card either by photocopying or writing it down from the front of the card or swiping it through a “reader.” Increased attention is necessary in the states and by the federal government limiting the access and use of this information. AAMVA members have recognized the need to address privacy concerns with the MRZ. In its *Driver’s License/Identification Card Security Framework*, AAMVA has recommended that all jurisdictions consider legislation limiting the use of information collected and used from the machine-readable portion(s) of a driver’s license and identification card.

Besides law enforcement, there are many other authorized users of the driver’s license and identification card, including DMVs. Encrypting the information denies many of these users, such as banks and retailers, the ability to ensure that the human readable information on the front of the card matches what is carried in the MRZ. Fraudulent credentials have been uncovered in this manner, and encryption literally denies this measure of security. Encryption does not provide the benefits those outside the motor vehicle community believe it does.

As law enforcement is a major user of the MRZ and many forces have invested funds in readers, encryption impedes this investment and time-saving process and could potentially undermine the states’ efforts to efficiently collect conviction data in a timely manner especially for programs monitored by the FMCSA. AAMVA members do not support any encryption efforts on the driver’s license or identification card.

Conclusion

About 100 years ago, states began to issue driver’s licenses to address one basic tenet; to attest to a person’s ability to drive. Those tenets have certainly changed over the years and the pure safety and driver credentialing mission has been distorted by many federal mandates and ancillary requirements. The federal government requires DMVs to be responsible for such on driver related functions as driver license suspensions for parents not paying court-ordered child support and for voter registration with “motor voter.” A host of other mandates are required by various state laws. And, most recently DMVs are responsible for the evolving tenet of the use of the driver’s license and identification card as the most commonly accepted form of identification in the U.S.

AAMVA’s members are used to change and challenge and adapting rapidly. AAMVA members are supportive of the concept of The REAL ID Act and its most basic intentions to continue to secure the driver’s license and identification card issuance process and to advance minimum standards. However, Congress and DHS must provide flexibility to the states, otherwise, the REAL ID will impede any state’s ability to continue to make progress to secure the driver’s licensing and identification card issuance process in a diligent and reasonable manner.

States have been and remain committed to increasing the security and integrity of their driver’s license and identification card issuance processes. AAMVA members are cognizant of the

critical need to continue to improve the driver's license and identification card issuance process and reduce fraud, Congress and DHS must recognize that the implications of implementation are far reaching. Many of those implications have not been adequately addressed in the NPRM. Applicant processing time will more than double for citizens in most states and wait times in some states will increase by up to 200 percent. The costs are astronomical. While the intentions are important, the Administration, DHS and Congress have continued to grossly underestimate the impact of the REAL ID Act.

We stand ready to work with Congress and DHS to improve the integrity of the driver's license and identification card while protecting personal information and maintaining privacy.

For more information, please contact Tom Wolfsohn, AAMVA's Chief Policy Officer at (703) 522-4200 or twolfsohn@aamva.org

STATEMENT OF

DR. JAMES JAY CARAFANO

SENIOR RESEARCH FELLOW
THE HERITAGE FOUNDATION214 MASSACHUSETTS AVENUE, NE
WASHINGTON, DC 20002

BEFORE THE SENATE COMMITTEE ON THE JUDICIARY

“Making REAL ID A Reality—Concerns, Challenges, Choices, Solutions”

(Delivered May 8, 2007)

Mr. Chairman and other distinguished Members, I am honored to testify before you today.¹ In my testimony, I want to make the case that national standards for identity credentials that are presented for a federal purpose make sense as a 21st century measure to help keep America safe, free, and prosperous.² These standards can be implemented in a manner that respects constitutionally guaranteed liberties and the principle of federalism; makes economic sense; better protects the individual liberties and privacies of US persons; and contributes to national security and public safety.

First, I would like to talk about what we should and should not do. *We should not institute anything like a universal national identity card.* Such a program would be unnecessary, extraordinarily expensive, and inefficient. A national ID card would provide little real additional security and would be found, rightfully, troubling to most Americans. On the other hand, an absence of national standards in the face of the current onslaught of efforts to obtain or falsify identity documents for criminal and other malicious purposes makes no sense in the 21st century.

Second, I would like to address the concerns and challenges facing the implementation of national standards.

¹ The title and affiliation are for identification purposes only. Staff of The Heritage Foundation testify as individuals. The views expressed are our own and do not reflect an institutional position for The Heritage Foundation or its board of trustees. The Heritage Foundation is a public policy, research, and educational organization. It is privately supported, receives no funds from government at any level, and performs no government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During the past two years, it had approximately 275,000 individual, foundation, and corporate supporters representing every State in the nation. Its 2005 contributions came from the following sources: individuals (63%), foundations (21%), corporations (4%), investment income (9%), publication sales and other sources (3%).

² These recommendations were first made in a Heritage Foundation Task Force report in January 2002. See Chapter 3 in L. Paul Bremmer III and Edwin Meese III, *Defending the American Homeland* (January 2002), at www.heritage.org/Research/HomelandDefense/upload/9709_1.pdf.

Third, I would like to outline a strategy for implementing national standards in a manner that is both efficient and effective, enhancing protection of both the freedom and the safety of all Americans.

In short, Congress should insist that the Administration fully implement the requirements for national standards in the Intelligence Reform and Terrorism Prevention Act of 2004 and the REAL ID Act of 2005. These laws do not create a national identification card, but establish that when key identification materials, such as drivers' licenses (and the documents used to obtain them, such as birth certificates), are issued at any level of government and used for a federal purpose (such as security checks before boarding commercial passenger planes), these documents must meet national standards of authenticity. Such documents should only be issued to persons lawfully living in the United States. To prevent tampering, counterfeiting, or fraud, and to enhance privacy protections the laws also establish standards security features concerning identification cards. Congress should not back-off the requirement for national standards and appropriate reasonable funds to help states establish systems to meet requirements under the REAL ID Act.

Winning the Long War

My principle concern with the implementation of REAL ID is in regard to the implications for national security and public safety. The security dangers of the 21st century are enduring challenges that requiring enduring solutions. Typically, in long wars, as states become desperate to win, they pull power to the center, centralize decision-making, increase taxation, and limit liberties. Ironically, as they became garrison states the effort to mobilize power made them less powerful. Less innovative, less productive, and less free, their wars became wars of attrition in which the states found themselves weakened at the end of the struggle—even if they were the winners. One of the notable exceptions to this historical trend was the United States and its allies during the Cold War, in which they emerged from the conflict stronger, more independent, and more free than when the contest started.³ The reason America weathered the Cold War so well was that it followed the tenets of good long war strategy.⁴ The Cold War was won by:

- *Providing Security.* It was important to take the initiative away from the enemy and to protect American citizens—therefore, the nation needed a strong mix of both offensive and defensive means. Nothing was to be gained by seeming weak and vulnerable in the eyes of the enemy.
- *Building a Strong Economy.* Americans realized early on that economic power would be the taproot of strength—the source of power that would enable the

³ See, for example, Aaron L. Friedberg, *In the Shadow of the Garrison State: America's Anti-Statism and Its Cold War Strategy* (Princeton, N.J.: Princeton University Press, 2000).

⁴ Described in James Jay Carafano and Paul Rosenzweig, *Winning the Long War: Lessons for the Cold War for Defeating Terrorism and Preserving Freedom* (Washington, D.C.: The Heritage Foundation, 2005).

nation to compete over the long term and would better the lives of its citizens. Maintaining a robust economy was a priority.

- *Protecting Civil Liberties.* Preserving a vibrant civil society and avoiding “the greatest danger”—the threat of sacrificing civil liberties in the name of security—was critical as well. Only a strong civil society gives the nation the will to persevere during the difficult days of a long war.
- *Winning the Struggle of Ideas.* From the beginning, Americans believed that in the end, victory is achieved because the enemy would abandon a corrupt, vacuous ideology that was destined to fail its people. In contrast, the West had a legitimate and credible alternative to offer. All America needed to do was face its detractors with courage and self-confidence.

The key to success was doing all four of these tasks with equal vigor, resisting the temptation to trade freedom for security or truth for prosperity. The United States could do worse than following the four principles of good protracted war strategy it practiced in the decades-long stand-off with the Soviet Union.

Identity, Freedom, and Security

The employment of identity cards as a security measure has implications for all four pillars of good long war strategy. A sound and principled program should help keep America safe, free, and prosperous.

Identity is one of the cornerstones of a free society. Verification of identity precludes more invasive intrusions into the lives and pursuits of average Americans. In a free society, many transactions, from cashing a check to boarding a plane, are predicated on an assumption that free citizens should be free to act as they choose under the rule of law. That is why criminals and terrorists work so assiduously to obtain identity instruments or the “breeder documents” (such as birth certificates) that are used to obtain identification cards.

Billions of dollars are lost each year due to identity theft, the fraudulent obtaining of government benefits, and other criminal activities. The exact amount is not known, but a typical example of the types of crimes perpetrated were the arrests made in New Jersey and Pennsylvania in 2003, breaking up a ring that withdrew \$10 million from individual bank accounts using phony driver’s licenses.⁵

There are security concerns as well. The September 11 hijackers, for example, obtained 17 driver’s licenses and 13 state-issued identifications. Some had duplicate driver’s licenses. This is unacceptable. Americans should neither have to sacrifice their ability to freely travel and openly conduct commerce, nor give up reasonable protections from malicious exploitation.

⁵ “Identity Thefts and Arrests,” *Privacy & American Business*, 10/5 (June/July 2003), p. 29.

The 9/11 Commission concluded that “the federal government should set standards for the issuance of birth certificates and sources of identification, such as driver’s licenses.” Congress acted. Both the Intelligence Reform and Terrorism Prevention Act of 2004 and the REAL ID Act of 2005 required national standards including:

- Requiring individuals obtaining driver’s licenses or personal identification cards to present documentation to establish identity, including U.S. nationality or lawful immigration status, and then verifying the validity of the documents;
- Establishing physical security features for ID cards to prevent tampering, counterfeiting, or fraud;
- Requiring standardized information on identity credentials, such as a full and complete name;
- Implementing security plans for state ID card issuance and computer systems, including employee background checks; and
- Ensuring that states share information to combat fraud and other criminal activity.

These are imminently practical and reasonable measures. In addition, they establish no new requirement for the federal government to obtain or maintain additional information on individual citizens, nor will the federal government issue, control, or manage the systems for issuing identity documents. Thus, requiring national standards cannot be construed as creating a national identity card. Finally, the requirement that states exchange data with each other and the federal government is neither unreasonable nor unprecedented. Forty-five states already have data-sharing agreements with each other.

National standards are not a silver bullet that will eliminate identity theft, fraud, counterfeiting or terrorism. On the other hand, implementing more secure documents and a more reliable issuance and management process will have tangible benefits. According to the American Association of Motor Vehicle Administrators, there are a number of distinct advantages to instituting national standards for security. These include:

- A reduction in driver’s license and identity fraud;
- A reduction in crime resulting from fraudulently obtained identification documents;
- Enhanced security and privacy of driver’s license information within and between motor vehicle agencies;
- Consistent minimum standards, policies, and procedures among motor vehicles agencies; and

- A climate of innovation, encouraging both technological and procedural advances in driver licensing.⁶

In contrast, I would argue that other proposals put before the Congress offer examples that far overstep the bounds of what is reasonable and practical. One of the most notable was the recommendation last year in both the Senate and House immigration reform bills that would have required a universal system to verify workplace eligibility for anyone wanting to get a job in the United States. Such a system would not only be extraordinarily expensive, impractical, and unnecessary, but would represent a major new intrusion into the lives of Americans, establishing an unprecedented centralized federal database of information on average citizens. There are far more cost-effective and practical means to enforce U.S. immigration and workplace laws.⁷ Indeed, centralized, federal programs that usurp the rights and responsibilities of states, local communities, the private sector, and individuals to look after themselves will *not* make us more safe, secure, and successful.

We are now faced with distinct choices. Developing intrusive, bureaucratic, and expensive national systems, such as national mandatory electronic workplace verification is overkill. On the other hand, abandoning national standards and returning to the pre-9/11 world in which criminals and terrorists can obtain or counterfeit identity documents with abandon makes no sense. They both represent courses we should not take. The requirements of REAL ID, in contrast, represent something sensible.

Concerns and Challenges

In the time since Congress acted, concerted efforts have been made to undermine REAL ID. These have included calling for further deferral of its implementation, demanding that the federal government spend tens of billions of dollars to upgrade state issuance facilities, trying to eliminate the requirement that citizenship or legal immigration status be validated, or even killing the whole program because of privacy concerns. None of these criticisms is warranted.

- Further postponing implementation will only encourage states to avoid making the investments needed to implement the law. Implementation has already been delayed until the end of 2009. This provides more than enough time to establish regulations to implement REAL ID and for states to undertake and fund the programs needed for them to do their part. In addition, this allows time to ensure that systems will be in place to allow states access to national databases in order to electronically verify the validity of required identification documents.

⁶ American Association of Motor Vehicle Administrators, *DL/ID Security Framework* (February 2004), p. 7, at www.aamva.org/aamva/DocumentDisplay.aspx?id=%7B25BBD457-FC4F-4852-A392-B91046252194%7D.

⁷ James Jay Carafano, "Workplace Enforcement to Combat Illegal Migration: Sensible Strategy and Practical Options," *Heritage Lecture No. 957*, July 26, 2006, at www.heritage.org/Research/NationalSecurity/hl957.cfm.

- Expecting the federal government to foot the bill for states that continually fail to provide their citizens with secure IDs, states that rely on antiquated systems, inadequately trained and supervised personnel, procedures that compromise security and fail to safeguard the privacy of individuals is wrong. REAL ID is less about adding new federal mandates than it is about encouraging states to properly shoulder their existing responsibilities. In addition, it should be noted that any costs involved in implementing reasonably secure standard identification cards will be more than recouped by the contribution that secure IDs make to facilitating travel and commerce while combating criminal exploitation of the freedoms of a free society.
- Eliminating the requirement for states to certify citizenship or lawful residence status undermines the central purpose of REAL ID—the presumption that the holder of the identity is acting lawfully.
- Raising the specter of privacy concerns is disingenuous. The law does not give the government more access to personal information, nor does it create a national data base. In fact, the law *adds* privacy protections such as requiring more security and background checks for government employees who handle personal data. In addition, the argument that identity theft will become more pervasive and serious because states have greater capacity to exchange data and thus identity thieves could potentially have more access to data to steal is not persuasive. Existing technology, including firewalls and intrusion detection software, can be employed to address these concerns. It is true that REAL ID is not a panacea for addressing privacy concerns. Even states that comply with national standards will not close every security loophole. For example, some states may issue cards that are vulnerable to “skimming” of digital information recorded on the card or they may have “open records” laws that provide greater opportunities for individual data to be obtained for malicious purposes. These vulnerabilities, however, should be addressed by state governments and legislators. Indeed, federal rules should not be overly prescriptive, allowing states to adopt best practices and business and technological innovations.

The Way Ahead

Congress and the Administration need a strategy to jump-start REAL ID. Specifically, they should:

- Not expect states to use funds from homeland security grants to implement REAL ID: That is just “robbing Peter to pay Paul.” Homeland security grants are meant to help build a national preparedness and response system. Congress should therefore appropriate specific funds for REAL ID, with the federal government paying its fair share of the costs of implementation.
- Focus federal dollars on the states closest to implementing REAL ID. This will show that the initiative *can* work and demonstrate the benefits of the program.

- Work with states that want to ensure that their driver's licenses meet federal standards under the Western Hemisphere Travel Initiative so that they can be used instead of passports for travel between the U.S., Canada, and Mexico. This will make REAL ID even more beneficial for states whose citizens frequently drive across the border.

Right for America

The 9/11 Commission made the case that state driver's licenses need to become a more secure credential. Congress acted—twice, passing laws to establish national standards. Now this common-sense initiative is under attack and may never be implemented. Congress and the Administration must act decisively to make the REAL ID program a reality. They need a strategy that encourages states with the capacity to implement REAL ID to do so quickly, demonstrating its viability and value. Once REAL ID is underway, momentum will build for other states to join; their citizens will not want to be left out of a program that materially contributes to their safety, their prosperity, and the protection of individual freedoms.

REAL ID is the right answer at the right time. The alternatives are stark. One is to continue to live in the “wild West,” where documents are counterfeited or exploited at will, costing the economy billions of dollar, disrupting the lives of millions, and putting all citizens at greater risk. The other is a national identity card that will cost many times the expense of implementing REAL ID and that really will be an additional intrusion into the lives of all Americans. Compared to the options of doing nothing or putting “Big Brother” in charge, REAL ID offers a sensible and sound program for creating the secure identity documents that are needed to help keep American safe, free, and prosperous.

Statement for the Record of
Ari Schwartz, Deputy Director
Center for Democracy and Technology
before
The Senate Committee on the Judiciary
on
"Will REAL ID Actually Make Us Safer?
An Examination of Privacy and Civil Liberties Concerns"
May 8, 2007

Introduction

Chairman Leahy, Ranking Member Specter and members of the committee, thank you for holding this public hearing on the REAL ID Act. The Center for Democracy and Technology (CDT) is pleased to submit this statement for the hearing record to further inform the highly complex and controversial debate over REAL ID.

CDT is a non-profit public interest organization dedicated to preserving and promoting privacy, civil liberties and other democratic values on the Internet.¹ CDT has been an active participant in the discussion over driver's license reform.²

Summary

The Center for Democracy and Technology supports the goal of making driver's license and ID card issuance more secure and thereby making the cards more reliable identity credentials. However, DHS's proposed regulations confirm our fears that the REAL ID Act is fundamentally flawed.

The current implementation of REAL ID will not make us safer. Both the Act itself and the proposed implementing regulations place a heavy importance on the driver's license as an identifying document, while failing to adequately improve privacy and security. Left unchanged, this could lead to a host of new concerns.

We encourage the Subcommittee to use the Identification Security Enhancement Act of 2007 (S. 717) as a starting point from which to create a robust statutory framework that directs driver's license and ID card reform without compromising privacy and security.

¹ More information on CDT's mission, activities and diverse funding sources can be found at <http://www.cdt.org/about/>.

² Among other activities, CDT testified in front of the House Transportation Committee in September 2002 on the issue of driver's license reform <<http://www.cdt.org/testimony/020805schwartz.shtml>>. In January 2004, CDT released a report entitled "Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses" — <<http://www.cdt.org/privacy/20040200dmv.pdf>>. CDT Deputy Director, Ari Schwartz, served on the Negotiated Rulemaking to Develop Minimum Standards for Driver's Licenses and Personal Identification at the US Department of Transportation formed under Section 7212 of the Intelligence Reform and Terrorism Prevention Act and abolished under the REAL ID Act.

We also urge the Subcommittee to include real input from states, security experts, civil liberties groups and the public.

I. CDT Supports Drivers License Reform

As the committee focuses on the problems with REAL ID, it is necessary to recognize that the fundamental cause of strengthening driver's licenses/ID cards is an important component of the broader goal of making Americans safer.³ In particular, CDT has identified several specific areas for immediate reform:

- **Standardizing and verifying which source documents may be used to get a driver's license or ID card — Creating an adequate standard set of source documents that must be properly vetted before applicants can receive REAL IDs** is an important goal that the Intelligence Reform package and REAL ID both adequately addressed.
- **Requiring minimum security features for the cards themselves to deter tampering and counterfeiting** — Development of minimum security standards that are not tied to particular technologies and can be easily updated to adapt to new situations would help prevent creation of fraudulent driver's licenses and ID cards. The Intelligence Reform package and REAL ID both adequately addressed this issue.
- **Improving the security of the physical locations where cards are made and supplies stored to deter outsider fraud, and improving security measures to deter insider fraud such as employee background checks and strict access controls to information and supplies** — CDT has found that criminals regularly breach the physical security of local Motor Vehicle Administration sites in order to steal information about individuals and materials to protect the cards or to bribe officials at the DMVs. In a 2004 report, CDT released a list of the previous year's local news stories of fraud. Examples of some the more egregious cases included:
 - The entire 11-person staff of the Newark, New Jersey DMV office was fired after Investigators determined fraud was so rampant that no one could be trusted.
 - An identity theft ring in Oregon was found with a CD-ROM full of Oregon drivers' personal information, as well as casings and cards that could only have been taken from an Oregon Motor Vehicles Office. Officials say that they could point at least 40 cases of identity theft back to these thieves.
 - Thieves used a forklift to break into a Utah DMV and steal the office safe and computer equipment. It is not known how much personal information was taken.⁴

³ CDT has actively worked on the Markle Foundation Task Force which has, among other reports, suggested changes to create "Reliable Identification for Homeland Protection and Collateral Gains" that suggests further identification reforms beyond the driver's license <http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf>.

⁴ These examples are taken from CDT's 2004 report entitled "Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses" —

While this issue is partially addressed by REAL ID, the DHS NPRM does not adequately set minimum standards for DHS' review of the state security and privacy plans.

CDT believes that a greater focus on these areas to improve driver's license and ID card issuance would vastly improve security of the current system with little impact on privacy at a manageable cost.

II. REAL ID Fails to Adequately Protect Privacy and Security

In repealing Section 7212 of the Intelligence Reform Act, the Real ID Act actively set back driver's license reform. REAL ID, which unlike the Intelligence Reform Act did not follow regular order in Congress, ended a negotiated rulemaking, which would have ensured input from state, privacy, immigration, law enforcement and other interests. As a bi-partisan group of Senators noted when REAL ID was first included in the supplemental spending package:

“[B]y repealing a provision enacting a central recommendation of the 9/11 Commission, in favor of unworkably rigid federal mandates, [the REAL ID Act] would jeopardize an initiative that can make the nation safer from terrorist attack.”⁵

In fact, REAL ID included several ill-conceived provisions that put the privacy of individuals at risk while doing little to protect security.

Risks to privacy and security specifically flow from three key provisions in the REAL ID Act:

- Each state must “provide electronic access to all other States to information contained in the motor vehicle database of the State,”⁶
- Each state must “employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format,”⁷ and
- Each driver's license and ID card must contain a Machine Readable Zone (MRZ), which enables fast and easy collection of personal information by digital means.⁸

<<http://www.cdt.org/privacy/20040200dmv.pdf>>. In all, CDT found 23 cases of publicly reported fraud in 15 different states. Because law enforcement was reluctant to give actual numbers of illegal license created, CDT could only give an estimate of tens of thousands of fraudulent licenses and dozens, if not hundreds, of related cases of identity theft.

⁵ REAL ID ACT Drivers' License Provisions Are Not Only Unworkable But Could Make Nation Less Safe; *Sununu, Lieberman, Alexander, and Durbin Present Facts; States Oppose Rigid Mandates* Press Release April 14, 2005—<http://lieberman.senate.gov/newsroom/release.cfm?id=236426&&>

⁶ REAL ID Act of 2005, Title II [H.R. 1268] Public Law 109-13, §202(d)(12).

⁷ §202(d)(1).

⁸ §202(d)(9).

The threats to civil liberties in these provisions can best be examined by looking at DHS' proposed implementation of the law.

III. DHS' Proposed Regulations Further Threaten Privacy and Security

It is clear that the privacy and security shortfalls found in the proposed regulations stem directly from those in the Act itself: the statutory language provides no guidance on privacy and little guidance on security. Still, CDT had hoped that DHS would see the clear connection between protecting privacy and protecting security in an identity system that contains (and even creates) so much personally identifiable information. Yet, rather than addressing our privacy concerns, DHS exacerbated many of them.

DHS states in the preamble to the draft regulations that it has addressed privacy "within the limits of its authority under the Act."⁹ The Department explains that the REAL ID Act "does not include statutory language authorizing DHS to prescribe privacy requirements," which "is in sharp contrast with the express authorization provided in section 7212 of IRTPA [Intelligence Reform and Terrorism Prevention Act of 2004], which was the prior state licensing provision repealed by the REAL ID Act."¹⁰

While DHS did take certain steps to help states safeguard information, the Act's structure and DHS' leaning against specific privacy requirements and metrics led to several policy decisions that put privacy and security of individuals at risk. In particular:

- **The Requirement for "Electronic Access" Is Overbroad** – The Act mandates that each state give every other state "electronic access" to information contained in its DMV database. A nationally accessible network of government databases that contain highly sensitive personal information creates increased potential for abuse by government and identity thieves. The "electronic access" mandated by the Act is far broader than what is necessary to achieve the goal of "only one license for one driver." *CDT recommends that the "electronic access" provision of the REAL ID Act be repealed.*

- **The Act and Regulations Seem to Be Leading to a Centralized ID Database** – To implement the "electronic access" provision of the Act, DHS officials have suggested that they will use a pointer database. While CDT has been told that the structure of this database will not be included in the Final Rule, several officials have suggested that it will be based upon the system used for commercial drivers: the Commercial Driver's License Information System (CDLIS), which is managed by the non-profit American Association of Motor Vehicle Administrators (AAMVA). Even though DHS and other proponents of REAL ID have repeatedly stated that the Act would not produce a centralized ID system, that is precisely what CDLIS is: a central database that houses a small but very significant amount of personal information (including name and Social Security Number)¹¹ and that links to other information contained in state databases.

⁹ Notice of Proposed Rulemaking (NPRM), Preamble at 10824-25.

¹⁰ NPRM, Preamble at 10825 n.3.

¹¹ See AAMVA's webpage on CDLIS <<http://www.aamva.org/TechServices/AppServ/CDLIS/>>.

Applying this system to all non-commercial drivers and ID card holders (i.e., virtually all U.S. residents) opens the door to the national linking of many other state and federal government databases; once a centralized identification database is established, there are no limits on what information it could point to. It is also important to note that, despite the fact that it is a national database, funded by the US Department of Transportation (DOT), CDLIS is not covered by the Privacy Act of 1974 because DOT views it as owned and operated by AAMVA.¹² Both the REAL ID Act and the proposed regulations fail to place any limits on the use of a central database. *CDT recommends that a central database not be created, and instead that a system be designed that gives a simple “yes” or “no” answer regarding whether a person already holds a driver’s license or ID card issued by another jurisdiction, where that information comes directly from each state and not via a central repository.*

• **The Act and Regulations Fail to Protect the Privacy and Security of Personal Data in State DMV Databases** – The Act requires states to digitally copy and store for several years all source documents, which contain highly sensitive personal information. But neither the Act nor the proposed regulations contain limitations on what personal information (including source documents) in a DMV database can be accessed, by whom, and for what purposes. *CDT recommends that source documents and other personal data in the state databases be accessible only by DMV officials for legitimate administrative purposes, and only by law enforcement officials for legitimate law enforcement purposes consistent with existing law. CDT recommends that there be specific minimum security requirements for personal data stored in DMV databases.*

• **The Act and the Regulations Fail to Build Security into the Machine Readable Zone Technology** – The Act mandates that each driver’s license and ID card have a machine-readable zone (MRZ) containing personal information, but the Act does not state what security and privacy standards the technology must meet. The Act seems to assume that the MRZ is, by itself, a security feature. In fact, the MRZ is really a convenience feature to allow DMVs and law enforcement to read the card quickly. The lack of statutory guidance enables DHS to endorse technology with weak security that will put personally identifiable information at greater risk by making it much easier to steal. In fact, the Preamble to the proposed regulations contemplates that some driver’s licenses and ID cards could contain an RFID chip so that they can be used in place of a passport book or PASS card at U.S. land and sea borders under the Western Hemisphere Travel Initiative (WHTI),¹³ yet the RFID technology chosen for the PASS card is insecure. *CDT recommends that privacy and security criteria be mandated for the MRZ technology.*

• **The Act and the Regulations Set No Limits on the Amount and Nature of Data in the MRZ** – The Act does not limit the type or amount of personal information that can be digitally stored in the MRZ, and it appears from the Preamble to the proposed regulations that DHS gave little attention to the tradeoff of putting items of personal information,

¹² A full list of DOT Privacy Act Systems of Records is available at <<http://www.dot.gov/privacy/privacyactnotices>>. CDLIS is not on this list.

¹³ NPRM, Preamble at 10841-42.

such as name, in the MRZ. There is a significant risk that any data in the MRZ will be inappropriately “skimmed.” *CDT recommends that the contents of the MRZ be limited to the information necessary for law enforcement purposes, and, as we explain below, that all information be protected against unauthorized skimming.*

• **The Act and the Regulations Fail to Limit the Compilation of Travel and Activity Information by Government Agencies** – Neither the Act nor the proposed regulations prohibit REAL ID cards from being read by innumerable state and federal government agencies, which would create a vast and efficient surveillance system that enables widespread tracking of the movements and activities of virtually all U.S. residents. *CDT recommends that the MRZ be encrypted or otherwise designed so it can be read and/or personal data can be “skimmed” (as opposed to the card being visually inspected) only by DMV officials for legitimate administrative purposes, and by law enforcement officials for legitimate law enforcement purposes consistent with existing law.*

• **The Act and the Regulations Contain No Protections Against Skimming by Third Parties** – Neither the Act nor the proposed regulations prohibit the cards from being read and personal data “skimmed” by businesses or other non-governmental third parties to create profiles and fill databases with information about the activities and preferences of millions of U.S. residents. *CDT recommends that the MRZ be encrypted or otherwise designed so it can be read and/or personal data “skimmed” (as opposed to the card being visually inspected) only by DMV officials for legitimate administrative purposes, and by law enforcement officials for legitimate law enforcement purposes consistent with existing law.*

• **A Nationally “Unique” Identifier Can Become the New Social Security Number, With All the Risks of the SSN** – The proposed regulations refer to a “unique” card number and require that it be included in the MRZ. It is unclear whether this number would be unique nationally or state-by-state. A nationally unique number could be abused as happened with the Social Security Number. *CDT recommends that the driver’s license or ID card number not be standardized and unique across states, and that its use be expressly limited.*

All of these issues relate to those parts of the REAL ID Act and the proposed implementing regulations that go far beyond what is needed to make driver’s license and ID card issuance more secure. The key point is that the more personal information is collected, centralized (even if in a technically “decentralized” system) and shared, the greater the potential for abuse not only by government and businesses, but also by terrorists, identity thieves and other criminals.

Neither the Act nor the proposed regulations control what information may be collected or accessed, by whom (i.e., state and government agencies, business, and other third-parties), and for what purposes. The Act does not mandate privacy and it barely addresses security, and DHS has failed to fill the gaps left by the statute despite an extensive discussion in the Preamble. Thus CDT concludes that the Act must be repealed or substantially rewritten to include mandates that protect privacy and ensure security.

And whether or not corrective legislation passes both houses of Congress, Congress must use its oversight authority to ensure that DHS does everything in its power under the law to protect privacy and ensure security.

IV. Conclusion

National policy to improve driver's licenses and ID cards in a way that protects privacy and security is needed. The REAL ID Act, as it is written and currently being implemented, will not lead us to that policy.

Both the Act itself and the proposed implementing regulations fail to protect privacy while creating serious security gaps. Congress must repeal or substantially rewrite the Act if driver's license and ID card reform is to be effective.

###

DEPARTMENT OF HOMELAND SECURITY
DOCKET NO. DHS 2006-0030
Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and
Identification Cards Acceptable by Federal Agencies for Official Purposes

COMMENTS OF:

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

AND

[EXPERTS IN PRIVACY AND TECHNOLOGY]

STEVEN AFTERGOOD
PROF. ANITA ALLEN
PROF. ANN BARTOW
PROF. CHRISTINE L. BORGMAN
PROF. JAMES BOYLE
DAVID CHAUM
PROF. JULIE E. COHEN
SIMON DAVIES
WHITFIELD DIFFIE
PROF. DAVID FARBER
PHILIP FRIEDMAN
DEBORAH HURLEY
PROF. JERRY KANG
CHRIS LARSEN
PROF. GARY MARX
MARY MINOW
DR. PETER G. NEUMANN
DR. DEBORAH PEEL
STEPHANIE PERRIN
PROF. ANITA RAMASASTRY
BRUCE SCHNEIER
ROBERT ELLIS SMITH
PROF. DANIEL J. SOLOVE
PROF. FRANK M. TUEKHEIMER

MAY 8, 2007

TABLE OF CONTENTS

I. INTRODUCTION	1
II. REAL ID CREATES A NATIONAL ID SYSTEM.....	2
A. Americans Have Consistently Rejected a National ID System.....	2
B. REAL ID Is Not Voluntary	3
C. Regulations Create a De Facto National ID System.....	5
III. DHS HAS THE OBLIGATION TO PROTECT PRIVACY OF CITIZENS	6
A. Privacy Act Applies Under OMB Guidelines	8
B. Requirements of Notice, Access, Correction and Judicially Enforceable Redress Must Be Mandated	9
IV. REAL ID CARDS MUST NOT DENOTE CITIZENSHIP STATUS.....	12
V. STANDARDS FOR ID DOCUMENTS WOULD BURDEN MANY INDIVIDUALS	13
VI. DATA VERIFICATION PROCEDURES ARE BASED ON FAULTY PREMISES	14
A. DHS Relies on Verification Databases That Are Not Available.....	14
B. DMV Workers Cannot and Should Not Become Immigration Officials.....	16
VII. MINIMUM DATA ELEMENTS ON MRT MUST REMAIN MINIMUM	17
A. Access to Data Must Be Limited.....	18
B. Unfettered Data Access Threatens Individual Privacy	20
C. Use of RFID Technology Increases Vulnerability of Data	24
VIII. UNIFORM LICENSE DESIGN WOULD CAUSE DISCRIMINATION AGAINST NON-REAL ID CARDHOLDERS	28
A. Universal Design Would Foster Suspicion of Innocent Individuals	29
B. Official and Unofficial Purposes of REAL ID Must Not Be Increased.....	29
IX. EXPANDED DATA COLLECTION AND RETENTION INCREASES SECURITY RISKS	31
X. NATIONAL ID DATABASE WOULD INCREASE SECURITY VULNERABILITIES	33
A. Regulations Would Not Improve Our Security Protections.....	34
B. Regulations Would Increase National Security Threats	39
C. Even If Assumptions Granted, REAL ID Would Not Substantially Affect Identity Theft Crimes	41
D. Centralized Identification System Increases Risk of Identity Theft.....	43
XI. REAL ID HARMS VICTIMS OF DOMESTIC VIOLENCE AND SEXUAL ASSAULT	46
A. REAL ID Endangers Address Confidentiality	46
B. National Database Threatens Security of Victims of Abuse Crimes.....	50
C. Proposed Background Check Procedures Do Not Fully Protect Victims of Abuse Crimes.....	51
D. REAL ID Increases the Power Abusers Have Over Their Victims.....	52
XII. METASYSTEM OF IDENTIFICATION IS BETTER CHOICE.....	54
XIII. IMPLEMENTATION JUST NOT POSSIBLE UNDER CURRENT TIMELINE.....	56
XIV. REAL ID MUST BE REPEALED.....	57
XV. CONCLUSION	58

I. INTRODUCTION

By notice published on March 9, 2007, the Department of Homeland Security (“DHS”) announced it seeks to establish “minimum standards for State-issued driver’s licenses and identification cards that Federal agencies would accept for official purposes after May 11, 2008, in accordance with the REAL ID Act of 2005.”¹ Pursuant to this notice, the aforementioned group (“Coalition”) submits these comments to request the Department of Homeland Security recommend to Congress that REAL ID is unworkable and must be repealed. The REAL ID Act creates an illegal *de facto* national identification system filled with threats to privacy, security and civil liberties that cannot be solved, no matter what the implementation plan set out by the regulations.² And if REAL ID implementation does go forward, the protections of the Privacy Act of 1974 must be fully enforced for all uses of the data current and future. Agencies should not be permitted to assert any exemptions and individuals must be granted all rights, including the judicially enforceable right to access and correct their records and to ensure compliance with all of the requirements of the Privacy Act.

The problematic adoption of the law now under consideration is now well known. The REAL ID Act was appended to a bill providing tsunami relief and military appropriations, and passed with little debate and no hearings. It was passed in this manner

¹ Dep’t of Homeland Sec., *Notice of Proposed Rulemaking: Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 72 Fed. Reg. 10,819 (Mar. 9, 2007) [“REAL ID Draft Regulations”], available at <http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/07-1009.htm>; see generally, EPIC, *National ID Cards and the REAL ID Act Page*, http://www.epic.org/privacy/id_cards/; EPIC, *Spotlight on Surveillance, Federal REAL ID Proposal Threatens Privacy and Security* (Mar. 2007), <http://www.epic.org/privacy/surveillance/spotlight/0307>; Anita Ramasastry, *Why the New Department of Homeland Security REAL ID Act Regulations are Unrealistic: Risks of Privacy and Security Violations and Identity Theft Remain, and Burdens on the States Are Too Severe*, Findlaw, Apr. 6, 2007, available at <http://writ.news.findlaw.com/ramasastry/20070406.html>.

² Pub. L. No. 109-13, 119 Stat. 231 (2005).

even though Republican and Democratic lawmakers in the Senate urged Senate Majority Leader Bill Frist to allow hearings on the bill and to permit a separate vote on the measure.³ The senators said they believe REAL ID “places an unrealistic and unfunded burden on state governments and erodes Americans’ civil liberties and privacy rights.”⁴ The people could not speak during this rushed process. They are speaking now.

II. REAL ID CREATES A NATIONAL ID SYSTEM

Throughout the history of the United States, its people have rejected the idea of a national identification system as abhorrent to freedom and democracy. The REAL ID Act and the draft regulations to implement it create a *de facto* national identification system, and the Act must be repealed.

A. Americans Have Consistently Rejected a National ID System

When the Social Security Number (SSN) was created in 1936, it was meant to be used only as an account number associated with the administration of the Social Security system.⁵ Though use of the SSN has expanded considerably, it is not a universal identifier and efforts to make it one have been consistently rejected.⁶ In 1973, the Health, Education and Welfare Secretary’s Advisory Committee on Automated Personal Data Systems rejected the creation of a national identifier and advocated the establishment of significant safeguards to protect personal information. The committee said:

³ Press Release, S. Comm. on Homeland Sec. & Governmental Affairs, Twelve Senators Urge Frist To Keep Real ID Act Off Supplemental Appropriations Bill Sweeping Proposal Needs Deliberate Consideration (Apr. 12, 2005), available at http://www.senate.gov/%7Egov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=953&Month=4&Year=2005.

⁴ *Id.*

⁵ EPIC & PRIVACY INT’L, *PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND PRACTICE* 47 (EPIC 2004).

⁶ See Marc Rotenberg, Exec. Dir., EPIC, *Testimony and Statement for the Record at a Hearing on Social Security Number High Risk Issues Before the Subcomm. on Social Sec., H. Comm on Ways & Means*, 109th Cong. (Mar. 16, 2006), available at http://www.epic.org/privacy/ssn/mar_16test.pdf; EPIC page on Social Security Numbers, <http://www.epic.org/privacy/ssn/>.

We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems. What is needed is a halt to the drift toward [a standard universal identifier] and prompt action to establish safeguards providing legal sanctions against abuses of automated personal data systems.⁷

In 1977, the Carter Administration reiterated that the SSN was not to become an identifier. In Congressional testimony in 1981, Attorney General William French Smith stated that the Reagan Administration was “explicitly opposed to the creation of a national identity card.”⁸ When it created the Department of Homeland Security, Congress made clear in the enabling legislation that the agency could not create a national ID system.⁹ In September 2004, then-Department of Homeland Security Secretary Tom Ridge reiterated, “[t]he legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They said there will be no national ID card.”¹⁰ The citizens of the United States have consistently rejected the idea of a national identification system.

B. REAL ID Is Not Voluntary

Supporters of REAL ID point to the legislation, which says that State implementation is “voluntary.” However, States are under considerable pressure to implement REAL ID and citizens who fail to carry the new identity document will find it impossible to pursue many routine activities. The administration has also pursued a

⁷ Dep’t of Health, Educ. & Welfare, Sec’y’s Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (July 1973), available at <http://www.epic.org/privacy/hew1973report/>.

⁸ Robert B. Cullen, *Administration Announcing Plan*, Associated Press, July 30, 1981.

⁹ Pub. L. No. 107-296, 116 Stat. 2135 (2002).

¹⁰ Tom Ridge, Sec’y, Dep’t of Homeland Sec., *Address at the Center for Transatlantic Relations at Johns Hopkins University: “Transatlantic Homeland Security Conference”* (Sept. 13, 2004), available at http://www.dhs.gov/xnews/speeches/speech_0206.shtm.

heavy-handed assault on those who have raised legitimate questions about the efficacy, cost, and impact of the \$23B program. Critics of REAL ID have been labeled anti-security. In Congressional testimony, a high-ranking DHS official said, “Any State or territory that does not comply increases the risk for the rest of the Nation.”¹¹ It is not anti-security to reject a national identification system that does not add to our security protections, but in fact makes us weaker as a nation. This system is also an unfunded mandate that imposes an enormous burden upon the states and the citizenry. The federal government has estimated that REAL ID will cost \$23.1 billion, but it has allocated only \$40 million for implementation and has told the states that they may divert homeland security grant funding already allocated to other security programs for REAL ID.¹²

Design standardization means that anyone with a different license or ID card would be instantly recognized, and immediately suspected. The Department of Homeland Security already contemplates expanding the REAL ID card into “everyday transactions.”¹³ It will be easy for insurance firms, credit card companies, even video stores, to demand a REAL ID driver’s license or ID card in order to receive services. Significant delay, complication and possibly harassment or discrimination would fall upon those without a REAL ID card. In actuality, the “voluntary” card is the centerpiece of a *mandatory* national identification system that the federal government seeks to impose on the states and the citizens of the United States.

¹¹ Richard C. Barth, Ass’t Sec’y for Policy Development, Dep’t of Homeland Sec., *Testimony at a Hearing on Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers’ Licenses and Identification Cards Before the Subcomm. on Oversight of Gov’t Management, the Federal Workforce & the District of Columbia, S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. (Mar. 26, 2007) [“DHS Testimony at REAL ID Hearing”], available at http://hsgac.senate.gov/_files/Testimonybarth.pdf.

¹² REAL ID Draft Regulations at 10,845, *supra* note 1.

¹³ See Data Collection Expansion discussion, *infra* Section IX (DHS plans to expand uses of REAL ID).

C. Regulations Create a De Facto National ID System

The Department of Homeland Security draft regulations would (1) impose more difficult standards for acceptable identification documents that could limit the ability of individuals to get a state drivers license; (2) compel data verification procedures that the Federal government itself is not capable of following; (3) mandate minimum data elements required on the face of and in the machine readable zone of the card; (4) require changes to the design of licenses and identification cards (5) expand schedules and procedures for retention and distribution of identification documents and other personal data; and (6) dictate security standards for the card, state motor vehicle facilities, and the personal data and documents collected in state motor vehicle databases. These regulations create a *de facto* national identification system.

State licenses and identification cards must meet standards set out in the regulations to be accepted for Federal use. REAL ID cards will be necessary for: “accessing Federal facilities, boarding commercial aircraft, and entering nuclear power plants.”¹⁴ The Supreme Court has long recognized that citizens enjoy a constitutional right to travel. In *Saenz v. Roe*, the Court noted that the “‘constitutional right to travel from one State to another’ is firmly embedded in our jurisprudence.”¹⁵ For that reason, any government initiative that conditions the ability to travel upon the surrender of privacy rights requires particular scrutiny. This is particularly relevant under the REAL ID regulations, as they affect 245 million license and cardholders nationwide. REAL ID could preclude citizens from entering Federal courthouses to exercise their right to due

¹⁴ REAL ID Draft Regulations at 10,823, *supra* note 1.

¹⁵ 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).

process, or from entering Federal agency buildings in order to receive their Social Security or veterans' benefits.

DHS may compel card design standardization, "whether a uniform design/color should be implemented nationwide for non-REAL ID driver's licenses and identification cards," so that non-REAL ID cards will be easy to spot.¹⁶ This universal card design will lead to a national identification system, combined with the mandate under the proposed regulations imposing new requirements on state motor vehicle agencies so that the Federal government can link together their databases to distribute license and cardholders' personal data, create a national identification system.¹⁷ DHS also has considered expanding the official uses for the REAL ID system, going so far as to estimate that one of the ancillary benefits of REAL ID implementation would be to reduce identity theft – a reduction DHS bases on "the extent that the rulemaking leads to incidental and required use of REAL ID documents in everyday transactions."¹⁸ There are other ways in which DHS has contemplated expanding the uses of the REAL ID system so that the card becomes a national identifier – one card for each person throughout the country.¹⁹

III. DHS HAS THE OBLIGATION TO PROTECT PRIVACY OF CITIZENS

The Department of Homeland Security states that it is constrained in its power to protect the privacy of individuals and their data under the REAL ID Act. The agency claims in the notice of proposed regulations that "The Act does not include statutory

¹⁶ REAL ID Draft Regulations at 10,841, *supra* note 1.

¹⁷ *Id.* at 10,825.

¹⁸ Dep't of Homeland Sec., *Regulatory Evaluation; Notice of Proposed Rulemaking; REAL ID*; 6 *CFR* Part 37; *RIN: 1061-AA37; Docket No. DHS-2006-0030*, at 130 (Feb. 28, 2007) ["Regulatory Evaluation"], available at http://www.epic.org/privacy/id_cards/reg_eval_draftregs.pdf.

¹⁹ See Data Collection Expansion discussion, *infra* Section IX (DHS plans to expand uses of REAL ID).

language authorizing DHS to prescribe privacy requirements for the state-controlled databases or data exchange necessary to implement the Act.”²⁰ We agree with Sen. Joseph Lieberman, who stated, “The concept that federal agencies need explicit Congressional authorization to protect Americans’ privacy is just plain wrong. In fact, our government is obligated to ensure that programs and regulations do not unduly jeopardize an individual’s right to privacy.”²¹

The draft regulations include little in terms of privacy safeguards:

In summary, DHS has proposed the following privacy protections in its implementing regulations for the REAL ID Act: (1) The State-to-State data exchanges and the State data query of Federal reference databases will be State operated and governed; (2) as part of the State certification process, States will be required to submit a comprehensive security plan, including information as to how the State implements fair information principles; and (3) while acknowledging the benefits of employing encryption of the personal information stored on the identification cards, we invite comment on its feasibility and costs and benefits to ensure that its costs do not outweigh the benefits to privacy.²²

DHS’s statement that it is constrained in its ability to set privacy protections for the REAL ID system is a product of the agency’s mistaken belief that security and privacy are separate. Security and privacy are intertwined; one cannot have a secure system if privacy safeguards are not created, as well. DHS stated that it “believes that this language [in the REAL ID Act] provides authority for it to define basic security program requirements to ensure the integrity of the licenses and identification cards.”²³ Because DHS has the authority to define basic security requirements, it also has the authority to set basic privacy safeguards for the REAL ID system.

²⁰ REAL ID Draft Regulations at 10,825, *supra* note 1.

²¹ Joseph Lieberman, U.S. Senator, *Statement at a Hearing on Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers’ Licenses and Identification Cards Before the Subcomm. on Oversight of Gov’t Management, the Federal Workforce & the District of Columbia, S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. (Mar. 26, 2007).

²² REAL ID Draft Regulations at 10,826, *supra* note 1.

²³ *Id.*

The draft regulations create a national identification system that affects 245 million license and cardholders nationwide, yet DHS is hesitant to ensure strong privacy safeguards in the system itself. DHS has the obligation to protect the privacy of citizens affected by this system and must do more than the feeble attempts set out in the draft regulations.

A. Privacy Act Applies Under OMB Guidelines

The Department of Homeland Security states that the Privacy Act of 1974²⁴ applies to only one part of the REAL ID system – the Problem Driver Pointer System.²⁵ However, the Privacy Act of 1974 applies to the entire national identification system, under guidelines set out by the Office of Management and Budget (“OMB”) and the Department of Homeland Security itself.

The OMB guidelines explain that the Privacy Act “stipulates that systems of records operated under contract or, in some instances, State or local governments operating under Federal mandate ‘by or on behalf of the agency . . . to accomplish an agency function’ are subject to . . . the Act.”²⁶ The guidelines also explain that the Privacy Act “make[s] it clear that the systems ‘maintained’ by an agency are not limited to those operated by agency personnel on agency premises but include certain systems operated pursuant to the terms of a contract to which the agency is a party.”²⁷ The REAL ID system is operated under a Federal mandate to accomplish several agency functions, including immigration control.

²⁴ 5 U.S.C. § 552a.

²⁵ REAL ID Draft Regulations at 10,826, *supra* note 1.

²⁶ Office of Mgmt. & Budget, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28,948, 28,951 (July 9, 1975) [“OMB Guidelines”], available at http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf.

²⁷ *Id.*

The REAL ID system is covered by the Privacy Act under the Department of Homeland Security's own policies. In a policy guidance memorandum from the agency's Privacy Office, defines "DHS Information Systems" as "an Information System operated, controlled, or directed by the U.S. Department of Homeland Security. This definition shall include information systems that other entities, including private sector organizations, operate on behalf of or for the benefit of the Department of Homeland Security."²⁸ The national system of interconnected State databases is "operate[d] on behalf of or for the benefit" of DHS. The Privacy Office also states:

As a matter of DHS policy, any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien.²⁹

It is clear that, under both DHS and OMG guidelines, the REAL ID national identification system is a system of records subject to the requirements and protections of the Privacy Act of 1974.

B. Requirements of Notice, Access, Correction and Judicially Enforceable Redress Must Be Mandated

If the Department of Homeland Security creates this system, the agency must fully apply Privacy Act requirements of notice, access, correction, and judicially enforceable redress to the entire REAL ID national identification system. Though the States are asked to include provisions for notice, access, correction and redress, this is not enough. The Privacy Act protections must be mandated in the REAL ID implementation regulations.

²⁸ Privacy Office, Dep't of Homeland Sec., *Privacy Policy Guidance Memorandum 2* (Jan. 19, 2007), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

²⁹ *Id.* at 1.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that Federal agencies could collect and required agencies to be transparent in their information practices.³⁰ In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

“[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies.” Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.³¹

The Privacy Act is intended “to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]”³² It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that “the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies,” and recognized that “the right to privacy is a personal and fundamental right protected by the Constitution of the United States.”³³ It thus sought to “provide certain protections for an individual against an invasion of personal privacy” by establishing a set of procedural and substantive rights.³⁴

We support the Department of Homeland Security's requirement that the States must include in their “comprehensive security plan” an outline of “how the State will

³⁰ S. Rep. No. 93-1183 at 1 (1974).

³¹ *Doe v. Chao*, 540 U.S. 614, 618 (2004).

³² S. Rep. No. 93-1183 at 1.

³³ Pub. L. No. 93-579 (1974).

³⁴ *Id.*

protect the privacy of personal information collected, disseminated or stored in connection with the issuance of REAL ID licenses from unauthorized access, misuse, fraud, and identity theft” and that the State has followed the Fair Information Practices (these are practices, not principles, as listed in the draft regulations), which “call for openness, individual participation (access, correction, and redress), purpose specification, data minimization, use and disclosure limitation, data quality and integrity, security safeguards, and accountability and auditing.”³⁵ However, this is not enough. The agency must mandate minimum security and privacy safeguards, which the states should build upon, to protect individuals and their personal information. Also, there must be standards for the issue of redress. How will redress be adjudicated if one State includes erroneous information in an individual’s file and passes that information on to another State? Will the individual have to petition both States separately for redress? Will neither State process the redress, because each believes it to be the responsibility of the other? The right of redress must be judicially enforceable.

The right of redress is internationally recognized. The Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognize that “the right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard.”³⁶ The rights of access and correction are central to what Congress sought to achieve through the Privacy Act:

³⁵ REAL ID Draft Regulations at 10,826, *supra* note 1.

³⁶ The OECD Privacy Guidelines of 1980 apply to “personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.” Org. for Econ. Co-operation & Dev., *Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data*, OECD Doc. 58 final at Art. 3(a) (Sept. 23, 1980), reprinted in M. ROTENBERG ED., *THE PRIVACY LAW*

The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.³⁷

The Privacy Act requirements that an individual be permitted access to personal information, that an individual be permitted to correct and amend personal information, and that an agency assure the reliability of personal information for its intended use must be applied to the entire REAL ID national identification system. Full application of the Privacy Act requirements to government record systems is the only way to ensure that data is accurate and complete, which is especially important in this context, where mistakes and misidentifications are costly.

IV. REAL ID CARDS MUST NOT DENOTE CITIZENSHIP STATUS

DHS is considering using the REAL ID card in the Western Hemisphere Travel Initiative border security program. For the REAL ID card to be compliant under the program, it would need to include long-range RFID technology, discussed below, and “the State would have to ensure that the State-issued REAL ID driver’s license or identification card denoted citizenship.”³⁸ It cannot be stressed strongly enough: **REAL ID cards must not include citizenship status.** If REAL ID cards were to signify citizenship, there would be intense scrutiny of and discrimination against individuals who chose not to carry the national identification card and those who “look foreign.”

SOURCEBOOK 2004 395 (EPIC 2005). The OECD Privacy Guidelines require, among other things, that there should be limitations on the collection of information; collection should be relevant to the purpose for which it is collected; there should be a policy of openness about the information’s existence, nature, collection, maintenance and use; and individuals should have rights to access, amend, complete, or erase information as appropriate. *Id.*

³⁷ H.R. Rep. No. 93-1416 at 15 (1974).

³⁸ REAL ID Draft Regulations at 10,842, *supra* note 1.

V. STANDARDS FOR ID DOCUMENTS WOULD BURDEN MANY INDIVIDUALS

Under the REAL ID Act, States are required to obtain and verify documents from applicants that establish “(1) The applicant’s identity, through a photo identity document, or a non-photo identity document that includes full legal name and date of birth if a photo identity document is not available; (2) Date of birth; (3) Proof of SSN or ineligibility for an SSN; (4) The applicant’s address of principal residence; and (5) Lawful status in the United States.”³⁹ Under the regulations, the only documents that could be accepted by the states to issue these new identity cards would be: (1) valid unexpired U.S. passport or the proposed passport card under the Western Hemisphere Travel Initiative; (2) certified copy of a birth certificate; (3) consular report of birth abroad; unexpired permanent resident card; unexpired employment authorization document; (4) unexpired foreign passport with valid U.S. visa affixed; (5) U.S. certificate of citizenship; U.S. certificate of naturalization; or (6) REAL ID driver’s license or identification card (issued in compliance with the final regulations).⁴⁰

The difficult standards for acceptable identification documents would limit the ability of some individuals to get a state driver’s license. There are questions as to whether some citizens could produce these documents, among them Native Americans, victims of natural disasters, domestic violence victims, the homeless, military personnel, or elderly individuals.⁴¹ We applaud the Department of Homeland Security for attempting to resolve this problem by allowing the States to voluntarily create an exceptions process for extraordinary circumstances. However, though DHS set minimum standards for data

³⁹ *Id.* at 10,827.

⁴⁰ *Id.* at 10,827-28.

⁴¹ See Domestic Violence discussion, *infra* Section XI (how domestic violence victims will be harmed by the standards); see Data Verification discussion, *infra* Section VI (general problems with the standards).

collection, retention and documentation of the transaction, the agency did not set minimum standards for eligibility, length of process, or cost of process.⁴² DHS states that persons born before 1935 might not have been issued birth certificates, so they might be eligible for the exceptions process.⁴³ Otherwise, there is nothing that explains to either States or individuals how they could prove eligibility, how long the process would take (days, weeks, months or even years), or if they could even afford the cost of the exceptions process.

VI. DATA VERIFICATION PROCEDURES ARE BASED ON FAULTY PREMISES

The data verification procedures mandated by the draft regulations are based on faulty premises: DHS relies on non-existing, unavailable or incomplete databases and the mistaken belief that DMV workers can or should be turned into Federal immigration officers. Each assumption creates more problems in the Department of Homeland Security's attempt to create a fundamentally flawed national identification system.

A. DHS Relies on Verification Databases That Are Not Available

Under REAL ID, the states must verify applicant documents and data with the issuing agency. DHS states that, "[f]or individual States to verify information and documentation provided by applicants, each State must have electronic access to multiple databases and systems Secure and timely access to trusted data sources is a prerequisite for effective verification of applicant data."⁴⁴ Yet, beyond the national identification system created by the State-to-State data exchange, two of four verification systems required are not available on a nationwide basis and third does not even exist.

⁴² REAL ID Draft Regulations at 10,834, *supra* note 1.

⁴³ *Id.* at 10,822.

⁴⁴ *Id.* at 10,833.

The database systems the States are required to verify applicant information against are: (1) Electronic Verification of Vital Events ("EVVE"), for birth certificate verification; (2) Social Security On-Line Verification ("SSOLV"), for Social Security Number verification; (3) Systematic Alien Verification for Entitlements ("SAVE"), for immigrant status verification; and (4) a Department of State system to verify data from "U.S. Passports, Consular Reports of Birth, and Certifications of Report of Birth."⁴⁵

The only system that is available for nationwide deployment is SSOLV, and a survey of States by the National Governors Association found that even this database would need substantial improvements to be able to handle the workload that would be needed under REAL ID.⁴⁶ EVVE is currently in pilot phase and only five states are participating.⁴⁷ Yet DHS bases its requirements on the assumption that EVVE will be ready for nationwide expansion by the implementation deadline May 2008.⁴⁸ The executive director of the organization overseeing the database has announced that EVVE will not be ready by May 2008 and the system may not be ready by the extended implementation deadline of December 2009.⁴⁹

DHS admits that only 20 states are using SAVE, and that the planned connection between SAVE and another database for foreign student status verification (Student and Exchange Visitor Information System, "SEVIS") may not be completed by the

⁴⁵ *Id.* at 10,830-35; Electronic Verification of Vital Events ("EVVE") is also called Electronic Verification of Vital Event Records ("EVVER") in some federal documents.

⁴⁶ Nat'l Governors Ass'n, et. al, *The REAL ID Act: National Impact Analysis* (Sept. 19, 2006) ["Governors' Analysis"], available at <http://www.nga.org/Files/pdf/0609REALID.PDF>.

⁴⁷ Nat'l Ass'n for Public Health Statistics & Info. Systems, *Electronic Verification of Vital Events (EVVE)*, <http://www.naphsis.org/projects/index.asp?bid=403>.

⁴⁸ REAL ID Draft Regulations at 10,831, *supra* note 1.

⁴⁹ Eleanor Stables, *Multi-Billion Dollar Real ID Program May Be Stymied Due to \$3 Million Shortfall*, CQ, Mar. 15, 2007.

implementation deadline of May 2008.⁵⁰ The State Department system to verify passports and some reports of births has not even been created, but DHS bases its mandates on the assumption that the system “is eventually developed.”⁵¹

B. DMV Workers Cannot and Should Not Become Immigration Officials

Under the regulations, State DMV employees would need to authenticate license and identification card applicants’ source documents, which means the employees would be required to physically inspect the documents and “verify[] that the source document presented under these regulations is genuine and has not been altered.”⁵² These source documents are: (1) valid unexpired U.S. passport or the proposed passport card under the Western Hemisphere Travel Initiative; (2) certified copy of a birth certificate; (3) consular report of birth abroad; unexpired permanent resident card; unexpired employment authorization document; (4) unexpired foreign passport with valid U.S. visa affixed; (5) U.S. certificate of citizenship; U.S. certificate of naturalization; or (6) REAL ID driver’s license or identification card (issued in compliance with the final regulations).⁵³

State DMV employees would be required to verify these documents, including Federal immigration documents, though they have no training to do so. DHS contemplates this problem and seeks to solve it by requiring that DMV employees handling source documents undergo 12 hours of “fraudulent document recognition” training.⁵⁴ A review of the Social Security Administration found that staff had difficulty recognizing counterfeit documents, though it is their primary job to verify these

⁵⁰ REAL ID Draft Regulations at 10,833, *supra* note 1.

⁵¹ *Id.* at 10,832.

⁵² *Id.* at 10,850.

⁵³ *Id.* at 10,827-28.

⁵⁴ Regulatory Evaluation at 122, *supra* note 18.

documents before issuing SSN. For example, the Government Accountability Office review reported difficulty with detection of fraudulent birth certificates. In one case, a fake in-state birth certificate was detected, but “SSA staff acknowledged that if a counterfeit out-of-state birth certificate had been used, SSA would likely have issued the SSN because of staff unfamiliarity with the specific features of numerous state birth certificates.”⁵⁵ It is questionable how well State DMV employees would be able to spot fraudulent documents, especially documents as rarely seen as consular reports of birth abroad, with merely 12 hours of training when it is difficult for counterfeit documents to be spotted by federal employees whose primary job is verification of source documents. Also, if a State DMV employee determines that an applicant’s source documents are fraudulent, where could the applicant turn? No redress procedure has been created.⁵⁶

VII. MINIMUM DATA ELEMENTS ON MRT MUST REMAIN MINIMUM

Under REAL ID, the following amount of information, at a minimum, must be on the REAL ID card: (1) full legal name; (2) date of birth; (3) gender; (4) driver’s license or identification card number; (5) digital photograph of the person; (6) address of principal residence; (7) signature; (8) physical security features; (9) a common machine readable technology, with defined minimum data elements; and, (10) card issue and expiration date.⁵⁷ The REAL ID card will include a 2D barcode as its machine readable technology. To protect privacy and improve security, this machine readable technology must either include encryption, which is recommended by the DHS Privacy Office, or access must be limited in some other form. Leaving the machine readable zone open would allow

⁵⁵ Gov’t Accountability Office, *Social Security Administration: Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens, but Some Weaknesses Remain*, GAO-04-12 (Oct. 2003), available at <http://www.gao.gov/cgi-bin/getrpt?GAO-04-12>.

⁵⁶ See Privacy Act discussion, *supra* Section III.

⁵⁷ REAL ID Draft Regulations at 10,8435, *supra* note 1.

unfettered third-party access to the data and leave 245 million license and cardholders nationwide at risk for individual tracking.

A. Access to Data Must Be Limited

Under the required changes to the design of State licenses and identification cards, DHS states the card must include “[p]hysical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purpose” and “common [machine-readable technology], with defined minimum data elements.”⁵⁸ The Federal agency will require the use of a two-dimensional bar code, but will not require the use of encryption. Though Homeland Security lays out the privacy and security problems associated with creating an unencrypted machine readable zone on the license, it does not require encryption because there are concerns about “operational complexity.”⁵⁹

The Department of Homeland Security’s own Privacy Office has urged the use of encryption in REAL ID cards. In its Privacy Impact Assessment of the draft regulations, the Privacy Office supported encryption “because 2D bar code readers are extremely common, the data could be captured from the driver’s licenses and identification cards and accessed by unauthorized third parties by simply reading the 2D bar code on the credential” if the data is left unencrypted.⁶⁰ DHS says that, “while cognizant of this problem, DHS believes that it would be outside its authority to address this issue within

⁵⁸ *Id.* at 10,835.

⁵⁹ *Id.* at 10,826.

⁶⁰ Dep’t of Homeland Sec. Privacy Office, *Privacy Impact Assessment for the REAL ID Act 16* (Mar. 1, 2007) [“Privacy Impact Assessment of Draft Regulations”], available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf and http://www.epic.org/privacy/id_cards/pia_030107.pdf.

this rulemaking.”⁶¹ As we have previously stated, DHS has the obligation to protect the privacy of individuals from whom they collect data, and the agency should not abdicate this responsibility.⁶² Imposing a requirement for the States to use unencrypted machine readable technology renders the cardholder unable to control who receives her data.

If, however, the agency determines that it will not use encryption because of concerns about the complexity of public key regulation, there is another approach that would better protect the privacy of individuals than unfettered access to the machine readable zone. We suggest that no personal data be placed on the machine readable zone. Instead, place a new identifier that is unused elsewhere (*i.e.*, not the driver’s license number or Social Security Number). This unique identifier will “point” to the records in the national database. Access to the database can be controlled by password and encryption security, because it is easier to regulate public keys in this scenario. Also, the State should ensure that a new unique identifier is created each time the machine readable zone is renewed or reissued, in order to make the identifier less useful as an everyday ID number – people would not be forever linked to this identifier. This approach would improve data security and privacy.

It is possible to use a “pointer” system in the machine readable zone, because the REAL ID Act did not set out what minimum document requirements on the machine readable zone need to be. The Act reads, “(9) a common machine-readable technology, with defined minimum data elements.”⁶³ Also, in the draft regulations, DHS requests comments on “[w]hether the data elements currently proposed for inclusion in the

⁶¹ REAL ID Draft Regulations at 10,837, *supra* note 1.

⁶² See Privacy Act discussion, *supra* Section III (federal agencies have the obligation to protect the privacy rights of individuals from whom they collect information).

⁶³ Pub. L. No. 109-13, 119 Stat. 231, 312, § 202(b)(9) (2005).

machine readable zone of the driver's license or identification card should be reduced or expanded.”⁶⁴ We recommend against putting any personal data on the machine readable zone and only placing this unique identifier. In this way, access to the data can be more tightly controlled.

DHS is required to include security protections on the REAL ID card. Under the REAL ID Act, the card must include “(8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for any fraudulent purpose.”⁶⁵ If DHS does not seek to limit access to the data on the REAL ID card, then it is signaling that it is acceptable for third parties to download, access and store the data for purposes beyond the three official purposes set out in the draft regulations: “accessing Federal facilities, boarding commercial aircraft, and entering nuclear power plants.”⁶⁶ Though DHS has contemplated expanding the uses for the REAL ID card, such an expansion would harm both individual privacy and security and quickly turn the United States into a country where the national identification card is involuntarily carried by everyone.

B. Unfettered Data Access Threatens Individual Privacy

If personal data is placed on the machine readable zone of the REAL ID card, then access to this data must be limited or individual privacy will be threatened. Unlimited access to this data will allow unauthorized third parties to download, access and store the personal data of any REAL ID cardholder.

The REAL ID Act mandates that the REAL ID card include “(8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for

⁶⁴ REAL ID Draft Regulations at 10,842, *supra* note 1.

⁶⁵ Pub. L. No. 109-13, 119 Stat. 231, 312, § 202(b)(8) (2005).

⁶⁶ REAL ID Draft Regulations at 10,823, *supra* note 1.

any fraudulent purpose.”⁶⁷ Allowing universal access to personal data contained on the REAL ID card would facilitate identity theft and security breaches. In the privacy impact assessment of the draft regulations, the Department of Homeland Security Privacy Office urges encryption for the REAL ID machine readable zone. It explains that unsecured digital data raises the risk of “skimming,” where one “expos[es] the information stored on the credential to unauthorized collection.”⁶⁸ This risk is not theoretical, the Privacy Office says, because “[r]eaders for the 2D bar code are readily available for purchase on the Internet and at a very low cost, which permits unauthorized third parties to skim the information for their own business needs or to sell to other third parties.”⁶⁹ Such skimming is often done without the individual’s knowledge or consent.

A recent case illustrates the security threat posed by open access to personal data on a machine readable technology. Last month, New York prosecutors charged thirteen people in a counterfeiting ring where restaurant servers on the East Coast (from Connecticut to Florida) skimmed data from customers’ credit cards.⁷⁰ “They used small hand-held devices, about the size of a cigarette package that could be kept in a pocket, to record information encoded in the magnetic strips of credit cards.”⁷¹ For a year and a half, the illegally gathered data was used to create fake credit cards and buy merchandise that the criminals resold.⁷² The financial data was easily accessed, downloaded and misused by the criminals because anyone with a skimmer device was able to read the unprotected machine readable zones.

⁶⁷ Pub. L. No. 109-13, 119 Stat. 231, 312, § 202(b)(8) (2005).

⁶⁸ Privacy Impact Assessment of Draft Regulations at 14, *supra* note 60.

⁶⁹ *Id.*

⁷⁰ Anemona Hartocollis, *\$3 Million Lost to Fraud Ring, Authorities Say*, N.Y. Times, April 21, 2007.

⁷¹ *Id.*

⁷² *Id.*

Some States are already facing problems with unauthorized parties accessing license and ID card data. California, Nebraska, New Hampshire, and Texas have laws restricting the skimming of such data.⁷³ In November, the New Jersey Motor Vehicle Commission sent letters to bar, restaurant and retail organizations explaining that they must stop scanning and downloading their patrons' license data.⁷⁴ Such actions violate the state Digital Driver License Act, as well as the state and federal Drivers Privacy Protection Acts, according to the commission.⁷⁵ Yet at least one establishment expressed reluctance to stop downloading and storing their customers' personal data, even in the face of legal action from the State.⁷⁶ Today, different States have different ID cards with a variety of data and security features. Imagine what would happen if 245 million cards nationwide had personal data in the exact same open access format.

When a person hands over her license or ID card today, the data is not routinely downloaded and stored. A grocery store clerk or club bouncer usually merely looks at the card, verifies age or address, and then hands the card back to the individual. No transaction is recorded. However, universal access to the machine readable zone of the REAL ID card would allow the data to be downloaded, stored and transferred without the knowledge or permission of the individual cardholder. A digital transaction would be recorded and a digital trail could be created.

For example, let us follow Douglas Osborne for one weekend in the near future, if the national identification system is created and the machine readable zone left open for universal access. On Friday night, Doug went to Eighteenth Street Lounge at 8 p.m. with

⁷³ Privacy Impact Assessment of Draft Regulations at 15, *supra* note 60.

⁷⁴ Ian T. Shearn, *License scanning is illegal, state says*, Star-Ledger (NJ), Nov. 23, 2006.

⁷⁵ *Id.*

⁷⁶ *Id.*

four friends, where their REAL ID cards were scanned and their personal data accessed and stored. At 9:35 p.m., he went to Club Five with the same four friends, where their REAL ID cards were scanned and their personal data accessed and stored. On Saturday afternoon, Doug bought two six-packs of Harpoon beer at 12:27 p.m. at a Safeway in Capitol Hill, where Doug's REAL ID data was scanned and stored. On Saturday night, Doug and two friends took the 5:10 flight to Atlantic City, where their cards were scanned and their information stored.⁷⁷ At 11:37 p.m., Doug and his two friends checked into a hotel, where their ID cards were scanned and their data downloaded. On Sunday morning, one of Doug's friends bought cigarettes at a casino, and his REAL ID was scanned and his data stored at 11:04 a.m. The digital trail could continue indefinitely. Individuals could easily be tracked from location to location as they went about their daily lives. Add to the REAL ID trail the information that could be gleaned from individuals' credit card transactions, and you have complete consumer profiles for which many companies would pay dearly.

DHS must include in restrictions against the addition of data beyond that defined in the REAL ID Act. To allow additional data on the machine readable zone is to increase the likelihood of the REAL ID card becoming the default identification documents for everyday transactions; this would increase the incentive for third parties to gather and store individuals' data, and substantially increase the card's value to marketers and criminals. Expansion of the data collected, uses allowed, and users authorized would greatly increase both threats to the security and privacy of personal data.

⁷⁷ "Because REAL IDs use a common MRT, the Transportation Security Administration (TSA) considered requiring the use of machine readers on REAL IDs at airports. *At this time* TSA has rejected [the plan]" (emphasis added). Regulatory Evaluation at 58, *supra* note 18.

C. Use of RFID Technology Increases Vulnerability of Data

DHS contemplates using the REAL ID system as part of its Federal border security program and requested comments on how States could incorporate long-range radio frequency identification (“RFID”) technology into the REAL ID card so that it could be used as part of the Western Hemisphere Travel Initiative.⁷⁸ Many groups have urged against the use of RFID technology in identification documents. There are significant privacy and security risks associated with the use of RFID-enabled identification cards, particularly if individuals are not able to control the disclosure of identifying information. The Department of State recognized these security and privacy threats and changed its E-Passport proposal because of them; the Department of Homeland Security (“DHS”) has just abandoned a plan to include RFID chips in border identification documents because the pilot test was a failure; and both the Department of Homeland Security’s Data Privacy and Integrity Advisory Committee and the Government Accountability Office recently cautioned against the use of RFID technology in identification documents.

Privacy and security risks associated with RFID-enabled identification cards include “skimming” and “eavesdropping.” Skimming occurs when an individual with unauthorized RFID reader gathers information from an RFID chip without the cardholder’s knowledge. Eavesdropping occurs when an unauthorized individual intercepts data as it is read by an authorized RFID reader. In the absence of effective security techniques, RFID tags are remotely and secretly readable. Although the creation

⁷⁸ REAL ID Draft Regulations at 10,842, *supra* note 1; see EPIC, Spotlight on Surveillance, *Homeland Security PASS Card: Leave Home Without It* (Aug. 2006), <http://www.epic.org/privacy/surveillance/spotlight/0806/> (why the Western Hemisphere Travel Initiative’s proposed passport card creates security threats); EPIC’s Page on Radio Frequency Identification (RFID) Systems, <http://www.epic.org/privacy/rfid/>.

of a small, easily portable RFID reader may be complex and expensive now, it will be easier as time passes. For example, the distance necessary to read RFID tags was initially thought to be a few inches. In the now-abandoned pilot test, the Department of Homeland Security said, “reliable reads can be received from a few inches to as much as 30 feet away from the reader.”⁷⁹ Other tests also have shown that RFID tags can be read from 70 feet or more, posing a significant risk of unauthorized access.⁸⁰

Some attacks already have succeeded against so-called “strengthened” identification documents. In one case, a computer expert was able to clone the United Kingdom’s electronic passport by using a commercially available RFID reader (which cost less than \$350) and software that took him less than a couple of days to write.⁸¹ In assessing the new RFID-enabled U.S. passports, one expert cloned the RFID tag and another used characteristics of the radio transmissions to identify individual chips, and those researchers spent only a few weeks attacking the RFID-enabled passports.⁸²

Another security risk of RFID-enabled identification cards is that of clandestine tracking. An unauthorized RFID reader could be constructed to mimic the authorized signal and then be used to secretly read the RFID tag embedded in the identification card. The Government Accountability Office has highlighted this security problem unique to wireless technology:

The widespread adoption of the technology can contribute to the increased occurrence of these privacy issues. As previously mentioned, tags can be read by any compatible reader. If readers and tags become ubiquitous, tagged items

⁷⁹ Dep’t of Homeland Sec., *Notice with request for comments*, 70 Fed. Reg. 44934, 44395 (Aug. 5, 2005), available at <http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAIISdocID=021420363270+2+0+0&WAIISaction=retrieve>.

⁸⁰ See Ziv Kfir and Avishai Wool, *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems* (Feb. 22, 2005), available at <http://eprint.iacr.org/2005/052>; Scott Bradner, *An RFID warning shot*, Network World, Feb. 7, 2005.

⁸¹ Steve Boggan, *Special Report: Identity Cards: Cracked It!*, Guardian, Nov. 17, 2006.

⁸² Bruce Schneier, Opinion, *The ID Chip You Don’t Want in Your Passport*, Wash. Post, Sept. 16, 2006.

carried by an individual can be scanned unbeknownst to that individual. Further, the increased presence of readers can provide more opportunities for data to be collected and aggregated.⁸³

So long as the RFID tag or chip can be read by unauthorized individuals, the person carrying that tag can be distinguished from any other person carrying a different tag. Individuals, unlike commercial products with RFID tags, should have the right to control the disclosure of their identifying information.

The federal government should be fully aware by now of the problems raised by an insecure RFID scheme. In April 2005, EPIC, the Electronic Frontier Foundation, and other groups submitted comments urging the State Department to abandon its E-Passport proposal, because it would have made personal data contained in hi-tech passports vulnerable to unauthorized access.⁸⁴ After the Department of State received more than 2,400 comments on its notice for proposed rulemaking on RFID-enabled passports, many of which criticized its serious disregard of security and privacy safeguards, the agency said it would implement Basic Access Control in an attempt to prevent skimming and eavesdropping.⁸⁵ The use of RFID-enabled identification documents, without including Basic Access Control and other safeguards, contravenes the Department of State's incorporation of basic security features into new U.S. passports.⁸⁶

In 2005, DHS began testing RFID-enabled I-94 forms in its United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") program to track the entry and

⁸³ Gov't Accountability Office, *Report to Congressional Requesters: Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (May 2005), available at <http://www.gao.gov/new.items/d05551.pdf>.

⁸⁴ EPIC, EFF, et. al, *Comments on RIN 1400-AB93: Electronic Passport* (Apr. 4, 2005), available at http://www.epic.org/privacy/rfid/rfid_passports-0405.pdf.

⁸⁵ Dep't of State, *Notice of Proposed Rule*, 70 Fed. Reg. 8305 (Feb. 18, 2005), available at <http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-3080.htm>.

⁸⁶ See Kim Zetter, *Feds Rethinking RFID Passport*, *Wired*, Apr. 26, 2005; Eric Lipton, *Bowing to Critics, U.S. to Alter Design of Electronic Passports*, *N.Y. Times*, Apr. 27, 2005.

exit of visitors.⁸⁷ The RFID-enabled forms stored a unique identification number, which is linked to data files containing foreign visitors' personal data.⁸⁸ EPIC warned that this flawed proposal would endanger personal privacy and security, citing the plan's lack of basic privacy and security safeguards.⁸⁹ The Department of Homeland Security's Inspector General echoed EPIC's warnings in a July 2006 report. The Inspector General found "security vulnerabilities that could be exploited to gain unauthorized or undetected access to sensitive data" associated with people who carried the RFID-enabled I-94 forms.⁹⁰ A report released by the Government Accountability Office in late January identified numerous performance and reliability issues in the 15-month test.⁹¹ The many problems with the RFID-enabled identification system led Homeland Security Secretary Michael Chertoff to admit in Congressional testimony on February 9th that the pilot program had failed, stating "yes, we're abandoning it. That's not going to be a solution" for border security.⁹²

⁸⁷ Dep't of Homeland Sec., *Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry*, 70 Fed. Reg. 44934 (Aug. 5, 2005), available at <http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WALSdocID=021420363270+2+0+0&WALSaction=retrieve>.

⁸⁸ The data includes biographic information, such as name, date of birth, country of citizenship, passport number and country of issuance, complete U.S. destination address, and digital fingerscans. Dep't of Homeland Sec., *Notice of Availability of Privacy Impact Assessment*, 70 Fed. Reg. 39300, 39305 (July 7, 2005), available at

<http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05-13371.htm>.

⁸⁹ EPIC, *Comments on Docket No. DHS-2005-0011: Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry* (Dec. 8, 2005), available at http://www.epic.org/privacy/us-visit/100305_rfid.pdf.

⁹⁰ Dep't of Homeland Sec. Inspector Gen., *Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS (Redacted)* 7 (July 2006), available at http://www.dhs.gov/xoig/assets/mgmt/rpts/OIGr_06-53_Jul06.pdf.

⁹¹ Richard M. Stana, Dir., Homeland Sec. & Justice Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Terrorism, Tech., & Homeland Sec., S. Comm. on the Judiciary*, 110th Cong. (Jan. 31, 2007), available at <http://www.gao.gov/new.items/d07378t.pdf>.

⁹² Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Testimony at a Hearing on the Fiscal Year 2008 Dep't of Homeland Sec. Budget Before the H. Comm. on Homeland Sec.*, 110th Cong. (Feb. 9, 2007), available at http://www.epic.org/privacy/us-visit/chertoff_020907.pdf.

In Congressional testimony in March, a GAO official cautioned against the use of RFID technology to track individuals. “Once a particular individual is identified through an RFID tag, personally identifiable information can be retrieved from any number of sources and then aggregated to develop a profile of the individual. Both tracking and profiling can compromise an individual’s privacy,” the GAO said.⁹³ The GAO reiterated the many problems with the failed US-VISIT RFID project and expressed concern that, despite this failure, DHS endorsed the use of RFID in the Western Hemisphere Travel Initiative PASS Card.

In December, the Department of Homeland Security Data Privacy and Integrity Advisory Committee adopted a report, “The Use of RFID for Identity Verification,” which included recommendations concerning the use of RFID in identification documents.⁹⁴ The committee outlined security and privacy threats associated with RFID use similar to the ones discussed and urged against RFID use unless the technology is the “least intrusive means to achieving departmental objectives.”⁹⁵ It is clear that the costs of RFID technology outweigh its benefits, and it should not be used in identification documents.

VIII. UNIFORM LICENSE DESIGN WOULD CAUSE DISCRIMINATION AGAINST NON-REAL ID CARDHOLDERS

⁹³ Linda D. Koontz, Dir., Info. Mgmt. Issues, Gov’t Accountability Office, *Testimony Before the Subcom. on Homeland Sec., H. Comm. on Appropriations*, 110th Cong. (Apr. 14, 2007), available at <http://www.gao.gov/new.items/d07630t.pdf>.

⁹⁴ Dep’t of Homeland Sec., Data Privacy & Integrity Advisory Comm., *The Use of RFID for Human Identity Verification (Report No. 2006-02)* (Dec. 6, 2006), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.

⁹⁵ *Id.* at 2.

The Department of Homeland Security contemplates a universal design for compliant and non-compliant REAL ID cards.⁹⁶ A universal design, especially for a card including citizenship status, would cause irreparable harm, as it would foster suspicion of those who do not wish to carry the REAL ID card. Uniform design for a national identification card would also create an enormous security risk.

A. Universal Design Would Foster Suspicion of Innocent Individuals

The agency is considering a uniform REAL ID card design, asking for comments on “[w]hether DHS should standardize the unique design or color required for non-REAL ID under the REAL ID Act for ease of nationwide recognition, and whether DHS should also implement a standardized design or color for REAL ID licenses.”⁹⁷ Mandating distinct designs or colors for both REAL ID and regular licenses and identification cards and requiring non-REAL ID driver’s licenses or ID cards to have explicit “invalid for federal purposes” designations turns this “voluntary” card into a mandatory national ID card. It would divide the country into two – people with the REAL ID card and those without – and anyone with a different license or ID card would be instantly suspicious. Significant delay, complication and possibly harassment or discrimination would fall upon those who choose not to carry a REAL ID card.

B. Official and Unofficial Purposes of REAL ID Must Not Be Increased

According to DHS, State driver’s licenses and identification cards must meet standards set out in the regulations to be accepted for Federal use under REAL ID. Such Federal purposes include entering Federal facilities, boarding commercial aircraft, entering nuclear power plants, and “any other purposes that the Secretary shall

⁹⁶ REAL ID Draft Regulations at 10,841-42, *supra* note 1.

⁹⁷ *Id.* at 10,842.

determine,” but the limitation on use to the three enumerated purposes are “for the time being.”⁹⁸ The Department of Homeland Security, via the draft regulations and Homeland Security Secretary Michael Chertoff, contemplates expanding the use of the national identification system.

In the draft regulations, the agency seeks comments on “how DHS could expand [the card’s official purposes] to other federal activities.”⁹⁹ In a February speech, Secretary Chertoff said he envisioned the REAL ID licenses “do[ing] double-duty or triple-duty.”¹⁰⁰ These national identification cards would “be used for a whole host of other purposes where you now have to carry different identification.”¹⁰¹ The agency also may use the REAL ID card in the Western Hemisphere Travel Initiative program – if citizenship is denoted on the card and long-range RFID technology added.¹⁰²

In the agency’s economic analysis of REAL ID implementation, reducing ID theft is listed as one of the potential ancillary benefits of the national identification system. However, the agency says that the potential benefit would depend on a *vast expansion* of REAL ID uses from the three official purposes required in the draft regulations; DHS suggests what is needed is “incidental and required use of REAL ID documents in everyday transactions.”¹⁰³ DHS envisions that employers, social service agencies

⁹⁸ Regulatory Evaluation at 30, *supra* note 18.

⁹⁹ REAL ID Draft Regulations at 10,823, *supra* note 1.

¹⁰⁰ Michael Chertoff, Sec’y, Dep’t of Homeland Sec., *Remarks by Secretary Michael Chertoff at the National Emergency Management Association Mid-Year Conference* (Feb. 12, 2007), available at http://www.dhs.gov/xnews/speeches/sp_1171376113152.shtm.

¹⁰¹ *Id.*

¹⁰² See RFID Technology discussion, *supra* Section VII(c) (security and privacy risks inherent in RFID use), and Citizenship Designation discussion, *supra* Section IV (citizenship designation breeds discrimination).

¹⁰³ Regulatory Evaluation at 130, *supra* note 18; see Identity Theft discussion, *infra* at Section X(c) (why REAL ID will not reduce identity theft).

(including Medicare, Medicaid and student financial aid), firearm sellers and licensors, and election workers will all use this national identification system.¹⁰⁴

The official and unofficial uses of REAL ID must not be broadened. Such expansion would harm national security. As explained below, using a single card for many identification purposes would be the same as using one key for every lock.

IX. EXPANDED DATA COLLECTION AND RETENTION INCREASES SECURITY RISKS

Under REAL ID, the government would have easy access to an incredible amount of personal data stored in one national database (or, according to the DHS description, 56 State and Territory databases, each of which can access all of the others).¹⁰⁵ DHS claims that it is not expanding data collection and retention, but it is enlarging schedules and procedures for retention and distribution of identification documents and other personal data. This broad expansion of data collection and retention in a national database creates significant threats to privacy and security.

The agency makes two claims about the expanded data retention under REAL ID that we dispute: (1) “Most States already include this [extensive, personal] information in a machine readable technology,” and (2) “neither the Real ID Act nor these proposed regulations gives the Federal Government any greater access to information than it had before.”¹⁰⁶ Each claim is false: DHS is mandating the increase of both the type of documents that need to be retained and the length of data retention, and the agency will give both State and Federal governments greater access to the personal data.

¹⁰⁴ See National Committee for Voting Integrity, <http://votingintegrity.org/> and EPIC, *Spotlight on Surveillance, With Some Electronic Voting Systems, Not All Votes Count* (Sept. 2006), <http://www.epic.org/privacy/surveillance/spotlight/0307> (why requiring any voter identification card is a poll tax).

¹⁰⁵ Section 202(d)(12); (d)(13).

¹⁰⁶ REAL ID Draft Regulations at 10,824, *supra* note 1.

With the REAL ID national identification system, DHS imposes new requirements on State motor vehicle agencies. Each of the 56 interconnected databases must contain all data fields printed on driver's licenses and ID cards, and driver's histories, including motor vehicle violations, suspensions, and points on licenses.¹⁰⁷ The States are compelled to begin maintaining paper copies or digital images of important identity documents, such as birth certificates or naturalized citizenship papers, for seven to 10 years.¹⁰⁸ This is a significant expansion of the personal data previously reviewed or stored by State motor vehicle agencies.

Currently these identification documents are kept in a variety of places – the Social Security system, the immigration system, local courthouses – and it takes considerable effort to gather them all together. Under REAL ID, all of these identification documents – concerning, among other things, births, marriages, deaths, immigration, social services – are consolidated into one national database, accessible to at least tens of thousands of government employees nationwide, which would give the Federal and State governments greater access than before.

Security expert Bruce Schneier, EPIC and others have explained that it decreases security to have one ID card for many purposes, as there will be a substantial amount of harm when the card is compromised.¹⁰⁹ There is also the threat that REAL ID is ostensibly trying to protect against: forged identification cards. Investing so much trust into one card means that criminals will only have to forge one identification card. “No

¹⁰⁷ Section 202(d)(12); (d)(13).

¹⁰⁸ REAL ID Draft Regulations at 10,855, *supra* note 1.

¹⁰⁹ Melissa Ngo, Dir., EPIC Identification & Surveillance Project, *Prepared Testimony and Statement for the Record at a Hearing on “Maryland Senate Joint Resolution 5” Before the Judicial Proceedings Comm. of the Maryland Senate* (Feb. 15, 2007) [“EPIC Testimony at Maryland Senate”], available at http://www.epic.org/privacy/id_cards/ngo_test_021507.pdf.

matter how unforgeable we make it, it will be forged. We can raise the price of forgery, but we can't make it impossible. Real IDs will be forged," Schneier said.¹¹⁰ A national database full of identification documents, images and data would entice many kinds of criminals, including terrorists who seek to steal the identity of a "trusted" individual.

A national identification system would divide the United States into two groups: (1) "trusted good guys" who have the national ID card, and (2) "untrusted bad guys" who do not. But, Schneier has pointed out that there is a third category that appears – bad guys who fit the good guy profile. Upon the release of the draft regulations, Schneier said, "The REAL ID regulations do not solve problems of the national ID card, which will fail when used by someone intent on subverting that system. Evildoers will be able steal the identity – and profile – of an honest person, doing an end-run around the REAL ID system."¹¹¹ This national identification system inherently contains significant threats to individual privacy and national security.¹¹²

X. NATIONAL ID DATABASE WOULD INCREASE SECURITY VULNERABILITIES

In the best-case scenario, the creation of the REAL ID national identification system does nothing to improve our security protections. In the worst-case scenario, the REAL ID system will exponentially increase threats to our national security. DHS's cryptic economic analysis is based upon incredible assumptions about possible future terrorist attacks that REAL ID would supposedly prevent. The economic analysis also

¹¹⁰ Bruce Schneier, *Real-ID: Costs and Benefits*, BULLETIN OF ATOMIC SCIENTISTS, Mar./Apr. 2007

["Schneier Essay"], available at http://www.schneier.com/blog/archives/2007/01/realid_costs_an.html.

¹¹¹ Press Release, EPIC, After Long Delay, Homeland Security Department Issues Regulations For Flawed National ID Plan (Mar. 2, 2007) ["EPIC Press Release on REAL ID"], available at <http://www.epic.org/press/030207.html>.

¹¹² See National Database discussion, *supra* Section X (how universal identification systems increase security threats).

ignores indirect costs. The REAL ID system would harm national security by increasing risks of identity theft and fraud, and by diverting funds away from other security programs that have been proven effective.

A. Regulations Would Not Improve Our Security Protections

Quantitative risk assessments are characteristically limited by false or unverifiable assumptions, faulty modeling, and above all short-sighted local optimization that tends to ignore long-term implications and slippery-slope changes in the validity of the assumptions.¹¹³ The economic analysis in the Department of Homeland Security's Regulatory Evaluation conducts such a quantitative risk assessment, and falls victims to these faulty assumptions. The Regulatory Evaluation states:

The primary benefit of REAL ID is to incrementally increase U.S. national security by reducing the vulnerability to criminal or terrorist activity of federal buildings, nuclear facilities, and aircraft. The chances of a terrorist attack on such targets being successful would generally increase if identity documents that grant access to them are in the possession of the attackers. This is demonstrated by the fact that several of the 9/11 hijackers had false driver's licenses or fraudulently obtained driver's licenses in their possession at the time of that attack.¹¹⁴

The analysis goes on to say, "REAL ID is highly unlikely to impact the consequences of a successful attack, but it may impact, on the margin, the chance of a terrorist attack being attempted and succeeding."¹¹⁵ So, DHS is attempting to determine the marginal chance that REAL ID will lessen the chance of success or discourage the attempt of a terrorist attack. Setting aside the assumption that a lack of REAL ID cards would make it more difficult to succeed in a terrorist attack upon the United States, we turn to the

¹¹³ Peter G. Neumann, *Computer-Related Risks*, § 7.10, Risks in Risk Analysis, pp. 255-257 (Addison-Wesley 1995).

¹¹⁴ Regulatory Evaluation at 126, *supra* note 18.

¹¹⁵ *Id.* at 127.

mathematical formula that DHS uses to calculate the REAL ID system's presumed "primary benefit."

The annual risk that the U.S. faces with regard to a potential terrorist attack can be represented as the chance that an attack will successfully take place, multiplied by the consequences of that attack. This can be mathematically represented as $\Pi * K$, where Π is the annual chance of a successful attack and K is the consequences of an attack in monetary terms. Homeland security measures such as REAL ID impact either the chance or consequences of a successful attack, or both. REAL ID is highly unlikely to impact the consequences of a successful attack, but it may impact, on the margin, the chance of a terrorist attack being attempted and succeeding. Let ΠB be this chance prior to the introduction of REAL ID, and ΠA be the chance after REAL ID comes into effect. Then the security impact of REAL ID in the course of one year can be measured in dollar terms as $(\Pi B - \Pi A) * K$.¹¹⁶

So, DHS takes the probability of a successful terrorist attack without the REAL ID national identification system in place (ΠB) and **subtracts** the probability of a successful attack with REAL ID (ΠA); then they take the resulting number and **multiply it by** the cost to the United States of a successful terrorist attack. Understandably, DHS goes onto explain that such an evaluation is very difficult and full of uncertainty.

Let the cost of the REAL ID regulation, which has been estimated, be C . Then for REAL ID to be fully justified on national security grounds alone, it must be the case that its benefit is at least as great as its costs. The annual risk-reduction benefit of Real ID is $(\Pi B - \Pi A) * K$, and the sum of this benefit over ten years must equal Real ID's cost, C . If we can determine a dollar value for K , then we can measure the marginal impact that REAL ID must bring about on the probability of a successful terrorist attack on a federal target for it to be fully justified by its security benefit.¹¹⁷

DHS is attempting to determine if $(\Pi B - \Pi A) * K$, which is the annual risk-reduction benefit of REAL ID, over 10 years, is at least equal to C , which is the cost of REAL ID, which DHS has set at -- a discounted rate of -- \$17.2B. DHS goes on to explain that this formula is based on the assumption that another attack would affect us, in economic

¹¹⁶ *Id.* at 127.

¹¹⁷ *Id.*

terms, the same as September 11, 2001. DHS estimates another attack would cost the United States either \$63.9 billion (an estimate of the immediate impact incurred) or \$374.7B (an estimate of the immediate and longer run impact).¹¹⁸ Other assumptions:

We assume that terrorist groups are seeking to inflict another attack with consequences on the order of magnitude of 9/11. We also assume that they are engaged in a campaign such that in every year during the 10-year period over which the costs and benefits of REAL ID are being evaluated, there is a positive and identical probability of being successfully attacked. Under this assumption, the expected present value of the consequences of the terrorist campaign against the U.S. homeland equals the sum of the expected values of consequences in each particular year over the 10-year period 2007-16:

$$\Pi 2007 * K 2007 + (1-\delta) * \Pi 2008 * K 2008 + (1-\delta)^2 * \Pi 2009 * K 2009 + \dots + (1-\delta)^9 * \Pi 2016 * K 2016,$$

where δ is the discount rate and K is the monetary value of consequences in real 2006 dollars. Because we assume that Π and K do not change from year to year, this can be re-written as:

$$\Pi * K + (1-\delta) * \Pi * K + (1-\delta)^2 * \Pi * K + \dots + (1-\delta)^9 * \Pi * K,$$

or

$$D * \Pi * K, \text{ where } D \text{ equals } \{1 + (1-\delta) + (1-\delta)^2 + \dots + (1-\delta)^9\}.$$

This expression is the sum of the expected discounted annual consequences of a terrorist campaign against the U.S. homeland over a ten-year period. As noted earlier, Real ID is anticipated to bring about a reduction in the annual probability of a successful attack from $\Pi B - \Pi A$, and the security benefit of Real ID over the ten-year period is therefore $D * (\Pi B - \Pi A) * K$.¹¹⁹

The variable D represents the annual consequences of a terrorist campaign against the U.S. over a ten-year period. DHS multiplies D by $[(\Pi B - \Pi A) \text{ times } K]$, which is the annual risk-reduction benefit of REAL ID. DHS then sets this equation equal to the direct cost of the REAL ID national ID system. By solving this equation, DHS hopes to find the **marginal impact on security** that the REAL ID system must have in order to

¹¹⁸ *Id.* at 127.

¹¹⁹ Regulatory Evaluation at 128-29, *supra* note 18.

break even. For “Real ID to break even with respect to cost and expected security benefits, it must be the case that $D*(\Pi B - \Pi A)*K = C$, or $\Pi B - \Pi A = C/(D*K)$.”¹²⁰ So, to break even, we need $[D*(\Pi B - \Pi A)*K]$ **to be equal to** C, meaning that how much REAL ID will save us in economic terms must be equal to the cost of the REAL ID system. Or, stated another way, it must be that $\Pi B - \Pi A$, probability of a successful terrorist attack without the REAL ID national identification system in place (ΠB) **minus** the probability of a successful attack with REAL ID (ΠA), **is equal to** C, cost of REAL ID system, **divided by** [D, annual consequences of a terrorist campaign against the U.S. over a ten-year period, multiplied by K, cost to the United States of a successful terrorist attack].

Here is where it gets tricky. Assuming the cost of REAL ID to be \$17.2B and the cost of a successful 9/11-type terrorist attack to be \$374.7 billion long-term, the value of $C/D*K$, in 2006 dollars, is 0.61%. Therefore, for “REAL ID to be fully justified by its primary security benefit, it must bring about a marginal reduction in the annual chance of a successful 9/11-type attack of 0.61%.”¹²¹ If DHS only estimates the immediate impact, and assumes the cost of REAL ID to be \$17.2 billion and the cost of the attack to be \$63.9 billion, then the value of $C/(D*K)$ is 3.60%. “For REAL ID to be fully justified by its primary security benefit in immediate impacts alone, it must bring about a marginal reduction in the annual chance of a successful 9/11-type attack of 3.60%.”¹²²

After all of these head-scratching mathematical assumptions, there is no conclusion, because, as DHS explains, “[w]ithout further information on the absolute level of ΠB [the probability of a successful terrorist attack without the REAL ID national

¹²⁰ *Id.* at 129.

¹²¹ *Id.*

¹²² *Id.*

identification system in place], it is difficult to say whether 0.61% or 3.60% is a very large reduction in the chance of successful attack, or a more moderate reduction.”¹²³

Therefore, it is unknown, even with all of these assumptions, whether REAL ID would even marginally reduce the possibility of a successful terrorist attack.

DHS acknowledges that certain assumptions are used in this analysis, such as assumptions for the variable K, the impact or the cost to the U.S. economy of a terrorist attack, which DHS assumes would be of the same magnitude as September 11, 2001. However, there is little discussion about the variable C, the cost of the REAL ID system. There are two ways in which the figures used by DHS are faulty: 1) they underestimate the direct costs and 2) they ignore the indirect costs. Such indirect costs include the impact upon civil liberties, increased risk of identity theft and fraud, and the diversion of funds from other, effective security programs.¹²⁴ Both faulty assumptions make the variable C smaller, while DHS has assumed a very large number for K, so the cost of the REAL ID system would seem dwarfed in comparison to the cost of another terrorist attack, making REAL ID seem cost-effective even if it only has a marginal effect on the probability of another attack – an effect REAL ID would not have.

REAL ID does not add to our security protections, but in fact increases our security threats by diverting needed funds from other national security projects. The estimated cost of REAL ID implementation has spiraled. Before the Act’s passage in 2005, the Congressional Budget Office estimated its cost to be around \$100 million.¹²⁵ In September, the National Conference of State Legislatures released a report estimating the

¹²³ *Id.*

¹²⁴ See Identity Theft discussion, *infra* at Section X(c) (REAL ID increases risks for identity theft).

¹²⁵ Cong. Budget Office, *Cost Estimate: H.R. 418: REAL ID Act of 2005* (Feb. 9, 2005), available at <http://www.cbo.gov/showdoc.cfm?index=6072&sequence=0&from=6>.

cost to be \$11 billion over the first five years.¹²⁶ Now, the Department of Homeland Security has admitted that REAL ID will cost states and individuals from \$17.2 billion to \$23.1 billion over ten years.¹²⁷ Congress has appropriated only \$40 million for REAL ID implementation. The Department of Homeland Security now says that a state can use up to 20 percent of its Homeland Security Grant Program funding for REAL ID implementation, which total about \$100 million for 2007.¹²⁸ Implementation costs for the state of California alone would be about \$500 million.¹²⁹

Diverting Homeland Security Grant Program money to REAL ID means that funding originally budgeted by the states for other homeland security projects, including training and equipment for rescue and first responder personnel. Even if the states received \$100 million per year for 10 years, that would still amount to only \$1.04 billion in Federal funds, a fraction of the \$17.2 billion to \$23.1 billion price tag. The rest of the cost would be borne by states and their residents.

B. Regulations Would Increase National Security Threats

In a recent analysis of the REAL ID Act, EPIC Executive Director Marc Rotenberg explained that “[s]ystems of identification remain central to many forms of security. But designing secure systems that do not introduce new risks is proving more difficult than many policymakers had imagined.”¹³⁰ The theory that the REAL ID Act

¹²⁶ Governors’ Analysis, *supra* note 46.

¹²⁷ REAL ID Draft Regulations at 10,845, *supra* note 1.

¹²⁸ Press Release, Dep’t of Homeland Sec., DHS Issues Proposal for States to Enhance Driver’s Licenses (Mar. 1, 2007), available at http://www.dhs.gov/xnews/releases/pr_1172765989904.shtm.

¹²⁹ Cal. Dep’t of Motor Vehicles, *Report to the Legislature on the Status of the REAL ID Act*, at 3 (Dec. 15, 2006), available at http://www.dmv.ca.gov/about/real_id/real_id.pdf.

¹³⁰ Marc Rotenberg, Exec. Dir., EPIC, *Real ID, Real Trouble?*, COMMUNICATIONS OF THE ACM, Mar. 2006, available at http://www.epic.org/privacy/id_cards/mr_cacm0306.pdf.

will prevent terrorism is predicated on the belief that only “outsiders” have an intent to harm the United States. This theory is fundamentally flawed.

Security expert Bruce Schneier has explained the theory of identification-based security. “In theory, if we know who you are, and if we have enough information about you, we can somehow predict whether you’re likely to be an evildoer,” Schneier said.¹³¹ This is impossible, because you cannot predict intent based on identification, he said.¹³² There are threats from both sides. Terrorist acts have been committed by U.S. citizens, “insiders.” Oklahoma City bombers Timothy McVeigh and Terry Nichols were U.S. citizens. As was Unabomber Ted Kaczynski.

A recent case illustrates Schneier’s point. According to court documents, last month, two men entered restricted areas at an airport in Florida, bypassed security screeners and carried a duffel bag containing 14 guns and drugs onto a commercial plane.¹³³ They avoided detection, because they are airline baggage handlers who used their uniforms and legally issued identification cards.¹³⁴ Both men had passed Federal background checks before they were hired, according to a spokesman for Comair, the airline that employed the men.¹³⁵ This questions the assumption that more and broader background checks, such as those suggested in the draft regulations, would prevent insider attacks. There are other problems with the background checks, which will be discussed below.¹³⁶

¹³¹ Schneier Essay, *supra* note 110.

¹³² *Id.*

¹³³ Jim Ellis, *Feds: Bag Of Guns Smuggled Onto Plane*, Associated Press, Mar. 9, 2007.

¹³⁴ *Id.*

¹³⁵ *Id.*

¹³⁶ See Domestic Violence discussion, *infra* Section XI.

The baggage handlers were only investigated and caught after police received an anonymous tip.¹³⁷ If the airport had identification-neutral security systems, such as requiring all fliers go through metal detectors, then the men could not have walked past them. But the identification-based security system failed because it allowed some fliers to skip screening because they are presumed to have no evil intent, and the men transported weapons and contraband aboard a commercial flight. Creating a national identification system would have just as devastating consequences, but on a larger scale, because many more people would be presumed “trusted” or “untrusted” based upon their decision to carry or not carry the REAL ID card.

C. Even If Assumptions Granted, REAL ID Would Not Substantially Affect Identity Theft Crimes

The draft regulations list reducing identity theft as one of the benefits of the REAL ID national identification system.¹³⁸ However, the agency’s own economic analysis under its Regulatory Evaluation shows that, even if one grants DHS the economic assumptions it makes, overall identity theft crimes would only be reduced by 2.8 percent, at best.¹³⁹

First, it is important to note that the DHS Regulatory Evaluation does not list “Reduce Identity Theft” under any of the three categories of benefits – “monetized,” “annualized quantified, but unmonetized,” or “unquantifiable benefits” in the accounting statement for the draft regulations.¹⁴⁰ Actually, the only benefit listed is under “unquantifiable benefits,” and that is the claim that REAL ID would “incrementally increase U.S. national security.”

¹³⁷ Jim Ellis, *Feds: Bag Of Guns Smuggled Onto Planes*, *supra* note 133.

¹³⁸ REAL ID Draft Regulations at 10,837, 10,846, *supra* note 1.

¹³⁹ Regulatory Evaluation at 5, *supra* note 18.

¹⁴⁰ *Id.* at 7.

Second, the Regulatory Evaluation later lists “reducing identity theft” as a potential ancillary benefit.¹⁴¹ The economic analysis explains that:

REAL ID will only have the ability to impact those types of identity theft that require a drivers license for successful implementation, and only to the extent that the rulemaking leads to incidental and required use of REAL ID documents in everyday transactions, which is an impact that also depends critically on decisions made by State and local governments and the private sector.¹⁴²

The potential ancillary benefit depends on a *vast expansion* of REAL ID uses from the three official purposes required in the draft regulations. The economic analysis assumes that REAL ID would be used in “everyday transactions,” which would have a devastating affect on identity theft protections.¹⁴³ Setting aside that flawed assumption and focusing upon the economic analysis, there is little benefit to be found. If all of the agency’s assumptions are agreed to, including the belief that REAL ID cards would be used in everyday transactions, the Department of Homeland Security still finds that REAL ID would reduce by 10 percent only the 28 percent of ID theft crimes that “are likely to require the presentation of an identity document like a drivers license.”¹⁴⁴ Therefore, the REAL ID national identification system will reduce only 2.8 percent of all identity theft crimes, a savings of approximately \$1.6 billion total for the 2007-2016 period.¹⁴⁵ The Department of Homeland Security has estimated that REAL ID would cost \$23.1 billion for that period. Basic economic analysis finds that one ought not spend \$23.1 billion to create a national identification system that might reduce the cost of identity theft crimes by \$1.6 billion.

¹⁴¹ *Id.* at 126, 129-30.

¹⁴² *Id.* at 130.

¹⁴³ See Identity Theft discussion, *infra* at Section X(c) (REAL ID increases risks of identity theft).

¹⁴⁴ Regulatory Evaluation at 130, *supra* note 18.

¹⁴⁵ *Id.*

D. Centralized Identification System Increases Risk of Identity Theft

The draft regulations create a national identification system with a national database, and this creates an enormous security risk. EPIC and others have explained that it decreases security to have a centralized system of identification, one ID card for many purposes, as there will be a substantial amount of harm when the card is compromised.¹⁴⁶

The REAL ID Act mandates that States provide every other state with electronic access to information contained in their motor vehicle databases and each State database must contain all data fields printed on driver's licenses and ID cards, and driver's histories, including motor vehicle violations, suspensions, and points on licenses.¹⁴⁷ Yet, DHS claims that a national database will not be created because the regulations "leave[] the decision of how to conduct the exchanges in the hands of the States."¹⁴⁸ This mandatory "State-to-State data exchange" creates one huge national database containing the personal information of 245 million license and ID cardholders – a database that can be accessed at DMVs across the country.

Using a national ID card would be as if you used one key to open your house, your car, your safe deposit box, your office, and more.¹⁴⁹ "The problem is that security doesn't come through identification; security comes through measures – airport screening, walls and door locks – that work without relying on identification"; therefore,

¹⁴⁶ EPIC Testimony at Maryland Senate, *supra* note 109; see EPIC, *Comments to the Federal Identity Theft Task Force, P065410* (Jan. 19, 2007), available at http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf; EPIC page on Identity Theft: Its Causes and Solutions, available at <http://www.epic.org/privacy/idtheft/>.

¹⁴⁷ Section 202(d)(12); (d)(13).

¹⁴⁸ REAL ID Draft Regulations at 10,825, *supra* note 1.

¹⁴⁹ Melissa Ngo, Dir., Identification & Surveillance Project, EPIC, *Prepared Testimony and Statement for the Record at a Meeting on "REAL ID Rulemaking" Before the Data Privacy & Integrity Advisory Comm., Dep't of Homeland Sec.* (Apr. 14, 2007), available at http://www.epic.org/privacy/id_cards/ngo_test_032107.pdf.

a centralized system of identification would not increase national security, security expert Bruce Schneier has said.¹⁵⁰

A large data breach affects the confidence and trust of the public. People will recoil from systems that create privacy and security risks for their personal data. We have seen countless data breaches that have left the personal data of tens of millions of Americans vulnerable to misuse. Recently, almost 46 million credit and debit card numbers were stolen by hackers who accessed the computer systems at the TJX Companies over a period of several years, making it the biggest breach of personal data ever reported.¹⁵¹ The computer system breaches began in July 2005 but weren't discovered until December 2006 – the financial data of millions were exposed for 17 months.¹⁵² Last May, an information security breach by a Department of Veterans Affairs employee resulted in the theft from his Maryland home of unencrypted data affecting 26.5 million veterans, active-duty personnel, and their family members.¹⁵³ The laptop and an external hard drive contained unencrypted information that included millions of Social Security numbers, disability ratings and other personal information.¹⁵⁴ In February 2005, databroker Choicepoint sold the records of at least 145,000 Americans to a criminal ring engaged in identity theft.¹⁵⁵ Also that year, Bank of America misplaced back-up tapes

¹⁵⁰ EPIC Press Release on REAL ID, *supra* note 111.

¹⁵¹ TJX Cos., Annual Report (Form 10-K), at 8-10 (Mar. 28, 2007), *available at* <http://ir.10kwizard.com/download.php?format=PDF&ipage=4772887&source=487>.

¹⁵² *Id.* at 7.

¹⁵³ See EPIC's Page on the Veterans Affairs Data Theft, <http://www.epic.org/privacy/vatheft/>.

¹⁵⁴ Statement, Dep't of Veterans Affairs, A Statement from the Department of Veterans Affairs (May 22, 2006).

¹⁵⁵ Robert O'Harrow Jr., *ID Theft Scam Hits D.C. Area Residents*, Wash. Post, Feb. 21, 2005, at A01; see EPIC's Page on ChoicePoint, <http://www.epic.org/privacy/choicepoint/>.

containing detailed financial information on 1.2 million employees in the Federal government, including many members of Congress.¹⁵⁶

A centralized identification system would be a tempting target for identity thieves. If a criminal breaks the system's security, then the criminal would have access to the personal information of every single person in that database. If this one, centralized system is used across the nation, this would put hundreds of millions of people at risk for identity theft.

There is another significant security risk, besides that of attacks by unauthorized users, and that is of authorized users abusing their power.¹⁵⁷ A 2005 scandal in Florida highlights risks associated with large database systems. A woman wrote to a newspaper criticizing a Florida sheriff as being too fat for police work and condemning his agency's use of stun guns.¹⁵⁸ Orange County Sheriff Kevin Beary ordered staffers to use state driver's license records to find the home address of his critic.¹⁵⁹ The sheriff sent her a letter at her home address, and she reported being surprised that he was able to track her down so easily.¹⁶⁰ In a case in Maryland just last year, three people – including a Maryland Motor Vehicle Administration official – were indicted on charges of “conspiring to sell unlawfully produced MVA-issued Maryland identification cards.”¹⁶¹

The consumer harm that results from the wrongful disclosure of personal information is very clear. For the seventh year in a row, identity theft is the No. 1 concern

¹⁵⁶ Robert Lemos, *Bank of America loses a million customer records*, CNet News.com, Feb. 25, 2005.

¹⁵⁷ See Domestic Violence discussion, *infra* Section XI (abusers use their authorized access to stalk victims).

¹⁵⁸ *Called fat, sheriff tracks down reader*, Associated Press, Apr. 6, 2005.

¹⁵⁹ *Id.*

¹⁶⁰ *Id.*

¹⁶¹ *Fake ID Cards*, Wash. Post, Mar. 15, 2006, at B02.

of U.S. consumers, according to the Federal Trade Commission's annual report.¹⁶² Over 104 million data records of U.S. residents have been exposed due to security breaches since January 2005, according to a report from the Privacy Rights Clearinghouse.¹⁶³ A centralized system of identification creates a "one-stop shop" for identity thieves. Centralizing authority over personal identity into one database and one card increases both the risk of identity theft as well as the scope of harm when it occurs. The confidence and trust of consumers will fall when such a breach occurs; people will withdraw because of privacy and security questions.

XI. REAL ID HARMS VICTIMS OF DOMESTIC VIOLENCE AND SEXUAL ASSAULT

The REAL ID national identification system creates difficulties for many groups, and it has significant consequences for domestic violence and sexual assault victims.¹⁶⁴ The residential address requirements endanger the ability of victims of domestic violence, sexual assault, and other crimes to hide from their abusers. The background check provisions set out in the draft regulations do not fully protect these victims from their abusers. In fact, the REAL ID system would help abusers find and track their victims across the nation.

A. *REAL ID Endangers Address Confidentiality*

Currently, many States allow domestic violence victims and others to protect the confidentiality of their residential addresses. States have created formal Address Confidentiality Programs and states have also provided general measures of residential

¹⁶² Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), available at <http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf>.

¹⁶³ Privacy Rights Clearinghouse, *Chronology of Data Breaches*, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

¹⁶⁴ See EPIC's Page on REAL ID and Domestic Violence, http://www.epic.org/privacy/dv/real_id.html.

address privacy. The proposed regulations override these substantial protections, and the overrides must be removed from the final regulations. The government must not make it easier for abusers to find their victims.

State Address Confidentiality Programs are an important tool for protecting the safety of domestic violence and sexual assault victims. Currently 20 states have address confidentiality programs.¹⁶⁵ Generally, under such programs, domestic violence or sexual assault victims register with the secretary of State or their attorney general. The victim is provided an address with that State office, which forwards the mail received there to the enrollee's residential address. This State office address is used in official correspondence with the State, though businesses are not usually required to use it.

The REAL ID Act requires that driver's licenses include a person's "address of principal residence."¹⁶⁶ This requirement effectively destroys state address confidentiality programs. The recent Violence Against Women and Department of Justice Reauthorization Act ("VAWA") included a requirement for DHS to "consider and address" the needs of certain groups when the agency is "developing regulations or guidance with regard to identification documents, including driver's licenses,"¹⁶⁷ These groups include domestic violence and sexual assault victims who are entitled to be enrolled in State address confidentiality programs; whose addresses are entitled to be suppressed via court order or State or Federal law; or whose information is protected

¹⁶⁵ See, Nat'l Conference of State Legislatures, *States With Address Confidentiality Programs for Domestic Violence Survivors*, <http://www.ncsl.org/programs/cyfl/dvsurvive.htm> (listing 19 states, not including Maryland but including Illinois which is unfunded); See also, Maryland Safe At Home Address Confidentiality Program, <http://www.sos.state.md.us/ACP/Information.htm>.

¹⁶⁶ Pub. L. No. 109-13, § 202(b)(6), 119 Stat. 231, 312 (2005).

¹⁶⁷ Pub. L. No. 109-162, § 827, 119 Stat. 2960, 3066 (2005).

from disclosure according to Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act 1996.¹⁶⁸

In the draft regulations, DHS has not followed the VAWA requirement; instead, the agency has significantly reduced the protections afforded by these programs. The proposed regulations require that addresses of principal residence be placed on the face of the REAL ID card and include some exemptions from this requirement, such as one for those enrolled in Federal Witness Security Programs.¹⁶⁹ The regulations also exempt those who are enrolled in State address confidentiality programs.¹⁷⁰ This is not the same as creating an exemption for those who are “entitled to be enrolled in the programs, as stated under the Violence Against Women Act.” In its discussion of the proposed rule, DHS does propose to include an exemption for those who are “entitled to be enrolled” in state address confidentiality programs.¹⁷¹ DHS must include this exemption in the final regulations. It cannot be that, as currently stated under the draft regulations, only those actually enrolled in State Address Confidentiality Programs would be exempted from the requirement to display their residential addresses on the face of the REAL ID card. Many domestic violence and sexual assault victims who are entitled to enroll in State Address Confidentiality Programs are not actually enrolled, for a variety of personal, safety and logistical reasons. They should not be punished for not actually enrolling in the program.

In order to adequately “consider and address” the needs of those who are “entitled to be enrolled” in a State confidentiality program, DHS must permit States to allow those who are entitled to be, but are not in address confidentiality programs to be exempted

¹⁶⁸ Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 827, 119 Stat. 2960, 3066 (2005).

¹⁶⁹ REAL ID Draft Regulations at 10,854, *supra* note 1.

¹⁷⁰ *Id.* at 10,854.

¹⁷¹ *Id.* at 10,836.

from the address of principal residence requirement. DHS should allow individuals to affirm that they fear victimization and would benefit from address confidentiality. It would be problematic to burden State motor vehicle agencies with the determination of who is entitled to be enrolled in an address confidentiality program. States could rely on the affirmation, rather than making a determination of the merits of an individual's need for confidentiality. This would close the gap between those domestic violence and sexual assault victims who are "entitled to be enrolled" and those who are actually enrolled in State Address Confidentiality Programs.

Also, though the proposed rule exempts from the residential address requirement those whose addresses are "entitled to be suppressed under State or Federal law or suppressed by a court order," this statement should be clarified to include States that generally allow individuals to display on licenses and ID cards an address other than their principal place of residence.¹⁷² Several States generally allow non-residential addresses to be on driver's licenses. Currently, at least seven States permit an address other than a residential address to be listed on licenses or ID cards (California,¹⁷³ Florida,¹⁷⁴ Montana,¹⁷⁵ New Mexico,¹⁷⁶ Oklahoma,¹⁷⁷ Wyoming,¹⁷⁸ and Virginia¹⁷⁹). For example, under Virginia's law, an applicant may choose to list a post office box, business or residential address.¹⁸⁰ The applicant is still required to provide their residential address

¹⁷² *Id.* at 10,854.

¹⁷³ Cal. Veh. Code § 12811(a)(1)(A).

¹⁷⁴ Fla. Stat. Ann. § 322.14(1)(a).

¹⁷⁵ Mont. Code. Ann. § 61-5-111.

¹⁷⁶ N.M. Stat. Ann. § 66-5-15 (1978).

¹⁷⁷ Okla. Stat. Ann. tit. 47, § 6-111(A)(1).

¹⁷⁸ Wyo. Stat. Ann. § 31-7-115(a)(iii).

¹⁷⁹ Va. Code Ann. § 46.2-342(A1).

¹⁸⁰ *Id.*

for motor vehicle department records, but this residential address is not displayed on the license or ID card.¹⁸¹

Domestic violence survivors, other crime victims, or those generally interested in protecting their privacy avail themselves of these State laws to keep their addresses confidential. These laws are the only way that survivors can protect themselves in States that do not have formal address confidentiality programs – four of those listed do not (Montana, New Mexico, Virginia and Wyoming). These general address privacy laws are also the only way that those who fear victimization, but who do not formally qualify for State Address Confidentiality programs, can protect themselves.

Without this exemption allowing States to permit any individual to protect her privacy by listing a non-residential address, the victims of domestic violence and sexual abuse will also face the embarrassment of disclosing that they are victims anytime that their identification is shown. There are few exceptions from the residential address requirement, and anyone holding a REAL ID card without the residential address listed would immediately be placed into one of these few categories.

B. National Database Threatens Security of Victims of Abuse Crimes

The draft regulations require that States provide electronic access to their motor vehicle database information to all other States.¹⁸² Survivors who flee their abusers, crossing into different states, will be exposed if their abuser breaches the security of any one of these interconnected databases. An abuser with an associate inside a State DMV, law enforcement, or other agency with access to the State records would be able to track a victim as the victim moves across the country.

¹⁸¹ *Id.*

¹⁸² REAL ID Draft Regulations at 10,856, *supra* note 1.

The danger of negligent and accidental disclosures is increased by REAL ID, as substantially more government employees will have access to all motor vehicle records nationwide. One example of accidental disclosure occurred in Wisconsin earlier this year -- a police officer disclosed a victim's address, found in a DMV record to a stalker; the officer did not know that the victim had a restraining order against this.¹⁸³ This sort of inadvertence would happen much more frequently in a post-REAL ID world, as access to personal information is spread throughout the national identification system. Intentional breaches by outsiders or authorized insiders abusing their power would also have a wider scope. Past abuses exemplify what can be expected in a nationwide scale. For example, in Arizona, a police officer admitted to accessing motor vehicle records to find personal information on women he was romantically interested in, as well as co-workers.¹⁸⁴ If REAL ID is implemented, abusers and insiders would have access to records throughout the country and would be able to track their victims no matter where they flee.

C. Proposed Background Check Procedures Do Not Fully Protect Victims of Abuse Crimes

DHS proposes that certain government employees be subject to criminal history background checks, with certain offenses disqualifying employees from specific jobs related to the REAL ID national identification system.¹⁸⁵ Covered employees would be limited to those who could affect the recording of information, the manufacture of REAL ID cards, or the information displayed on a card.¹⁸⁶ Employees who can access the record information without the ability to edit it are not subject to the background check

¹⁸³ Kevin Murphy, *Officer's Actions will Cost 25,000*, GAZETTEEXTRA, Feb. 15, 2007, available at <http://www.gazetteextra.com/mezera021507.asp>.

¹⁸⁴ Michael Kiefer, *Officer Admits to Tampering; Databases Used to Check on Women*, ARIZONA REPUBLIC, April 6, 2006, at B3.

¹⁸⁵ REAL ID Draft Regulations at 10,855, *supra* note 1.

¹⁸⁶ *Id.* at 10,856.

requirement. This massive loophole greatly increases the security and privacy risks of domestic violence and sexual abuse victims, as significant damage can be done by unauthorized data disclosure. In order to safeguard against these threats, the broad category of those who have access to records should be shrunk, rather than increasing the category of those who are covered by the background check requirement.

The suitability criteria of the background check do not match the threat of stalkers and abusers. DHS proposes to use the permanent and interim disqualifying criteria in the Transportation Security Administration's background checks for maritime and land transportation security at 49 C.F.R. 1572.103.¹⁸⁷ The offenses include espionage, sedition, treason, making bomb threats, and crimes involving transportation security incidents.¹⁸⁸ Some of the offenses, such as fraud and misrepresentation -- including identity fraud -- are relevant to the risks of improper disclosure and access to the records.¹⁸⁹ However, crimes such as stalking, surveillance, harassment and domestic abuse are not in this list. These crimes must be added to the list of disqualifying offenses, so that the REAL ID system does not create a loophole permitting abusers access to a national database that would allow them to track their victims no matter where the victims moved.

D. REAL ID Increases the Power Abusers Have Over Their Victims

REAL ID's stringent document requirements will place more power in the hands of abusers. Fleeing domestic violence or sexual abuse can be a sudden and dramatic step. Victims' advocates often counsel their clients to prepare "safety plans," which include

¹⁸⁷ *Id.* at 10,856.

¹⁸⁸ 49 C.F.R. 1572.103(a).

¹⁸⁹ *Id.* at 1572.103(b)(2)(iii).

gathering key documents such as passports, visas, and birth certificates.¹⁹⁰ The proposed regulations limit the types of documents that can be used to prove identity, which create problems for many groups, including abuse victims.¹⁹¹ The draft regulations permit exceptions for those who do not have the required documents “for reasons beyond their control.”¹⁹² The exception requires that the records “visibly indicate” that alternative documentation was accepted and that a “full explanation” of the reason be included in the record.¹⁹³ Thus victims will face the embarrassment of having intimate details of the abuse they have suffered included in a national database accessible to thousands of government employees across the nation. The “for reasons beyond their control” exception must specifically include abuse victims, so that they may not be punished for leaving their abusers. The visible indication and “full explanation” included in the records should be limited to the statement that alternative documents were accepted “for reasons of personal safety,” so that victims need not expose the history of their abuse to anyone who could view their DMV records.

Another problem is that this “for reasons beyond their control” exception does not apply to those who must demonstrate lawful immigration status.¹⁹⁴ Under the draft regulations, the demonstration of lawful status would require documents that an abuser would likely have control over. Abusers of immigrants who are able to control their victims immigration documents will be able to control the victim’s ability to obtain a

¹⁹⁰ E.g., Oakland County Coordinating Council Against Domestic Violence, *Domestic Violence Handbook – Personalized Safety Plan*, at <http://www.domesticviolence.org/plan.html> (last visited Mar. 30, 2007) (“Items to take, if possible. . . Birth Certificates . . . Social security cards . . . Passports, green cards, work permits”).

¹⁹¹ REAL ID Draft Regulations at 10,852, *supra* note 1; see Data Verification discussion, *supra* Section VI (general problems with the standards).

¹⁹² REAL ID Draft Regulations at 10,852, *supra* note 1.

¹⁹³ *Id.*

¹⁹⁴ *Id.*

REAL ID card or license. The “for reasons beyond their control” exception must be extended to those victims who must prove lawful immigration status, so that the abusers cannot use these documents to trap their victims into staying in abusive situations. The exception permitting those who do not have access to documents to use alternative documentation should be extended to the proof of lawful immigration status. Here, also, the visible indication and “full explanation” included in the victims’ DMV records should be limited to the statement that alternative documents were accepted “for reasons of personal safety,” so that victims need not expose the history of their abuse to anyone and everyone who could view their DMV records.

XII. METASYSTEM OF IDENTIFICATION IS BETTER CHOICE

Once personal data has fallen into the hands of an identity thief, the potential for its misuse is proportionate to the extent that the information can be used for illegitimate authentication. We have already explained why a universal identifier will not improve security. Rather than promoting the use of universal identifiers, EPIC advocates the distribution of identity or an identity metasytem in which authentication is confined to specific contexts in order to limit the scope for potential misuse. The danger of a single identifier is that the harm will be magnified when it is compromised.

A system of distributed identification reduces the risks associated with security breaches and the misuse of personal information. For example, a banking PIN number, in conjunction with a bank card, provides a better authentication system because it is not coupled with a single, immutable consumer identity. If a bank card and PIN combination is compromised, a new bank card and PIN number can be issued and the old combination cancelled, limiting the damage done by the compromised data. Drawbacks of such

structures, including the possibility for the existence of multiple cards, are currently being addressed by the creation of an identity metasytem in which multiple identities can be loosely coupled within a single secure system.¹⁹⁵

Distributing identity in this way allows for different profiles to be used in different authenticating contexts. New profiles can be created as required within a single identity metasytem. Misuse is therefore limited to the context of the information breached, whether it is a single bank account, online merchant, or medical records.

Possibilities for data misuse can also be limited at the data collection stage. EPIC has previously called attention to the need for Web sites to stop storing customer credit card information.¹⁹⁶ Amassing large databases of credit card numbers creates an attractive target for potential identity thieves. Creating a national ID card under REAL ID also creates an attractive target for potential identity thieves – imagine having access to digital copies of “breeder” documents, such as certified birth certificates and SSN cards.

First and foremost, the best response is not to create a centralized identification system such as the one realized under REAL ID. Another simple response to identity theft is to require a PIN to be used in conjunction with all identification cards. A third response is to forbid third-party collection or storage of data from identification cards. An identity metasytem would further reduce the value of such aggregated database targets, because authenticators would be separate and distinct from all personally identifiable information.

Finally, technological measures can be used to improve the reliability of authentication while respecting consumer privacy. International research efforts are

¹⁹⁵ Kim Cameron, *The Laws of Identity*, Identity Weblog, Dec. 9, 2004, <http://www.identityblog.com/stories/2004/12/09/thelaws.html>.

¹⁹⁶ See EPIC's Page on Identity Theft: Causes and Solutions, <http://www.epic.org/privacy/idtheft/>.

currently underway to create authentication systems that preserve anonymity, and include the development of new privacy enhancing technologies for use in such schemes.¹⁹⁷

These privacy enhancing technologies allow for the separation of authentication and identification and are being deployed in response to security vulnerabilities. Such technologies may plug in to identity metasystems, such as Microsoft's CardSpace. While the default settings of CardSpace do not currently meet recognized standards for privacy preservation,¹⁹⁸ this model should be studied in detail.¹⁹⁹

XIII. IMPLEMENTATION JUST NOT POSSIBLE UNDER CURRENT TIMELINE

Two years after Congress rushed through passage of the REAL ID Act, the Department of Homeland Security announced on March 1 proposed regulations to create the REAL ID national identification system. The draft regulations were released about 14 months before the May 2008 implementation deadline. After enormous criticism from the public and the States, DHS extended the deadline, but not by much.

Comments on the draft regulations are due by May 8. DHS says it will review the public comments and take them into consideration for the final regulations, the release of which is expected in August or September.²⁰⁰ In the draft regulations, DHS says it

¹⁹⁷ See, e.g., Carlisle Adams, *Delegation and Proxy Services in Digital Credential Environments*, Presented at the 7th Annual Privacy and Security Workshop, *Your Identity Please: Identity Theft and Identity Management in the 21st Century* (Nov. 2, 2006), available at <http://www.idtrail.org/files/cacrwkshpdigcred02nov06.pdf>; Stefan Brands, *Non-Intrusive Cross-Domain Digital Identity Management*, Presented at Proceedings of the 3rd Annual PKI R&D Workshop (Apr. 2004), available at http://www.idtrail.org/files/cross_domain_identity.pdf; David Chaum, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, Presented at ITL Seminar Series, *Secret-Ballot Receipts: True Voter-Verifiable Elections*, Nat'l Inst. of Standards & Tech. (May 19, 2004); Paul Van Oorschot and S. Stubblebine, *Countering Identity Theft through Digital Uniqueness, Location Cross-Checking, and Funneling*, Fin. Cryptography & Data Sec. (2005), available at <http://www.scs.carleton.ca/~paulv/papers/pvoss6-1.pdf>.

¹⁹⁸ Stefan Brands, *User centric identity: boon or worst nightmare to privacy?*, Identity Corner, Nov. 17, 2006, <http://www.idcorner.org/?p=142>.

¹⁹⁹ See generally, NAT'L RESEARCH COUNCIL, *WHO GOES THERE? AUTHENTICATION THROUGH THE LENS OF PRIVACY* (Nat'l Academies 2003).

²⁰⁰ DHS Testimony at REAL ID Hearing, *supra* note 11.

“strongly encourages States to submit certification packages by October 1, 2007,” and sets a drop-dead date of February 10, 2008, for states to file these certification packages, which detail States’ plans to fulfill the obligations detailed in the final regulations.²⁰¹ These certification packages include a “comprehensive security plan for [each State’s] DMV offices and driver’s license storage and production facilities, databases, and systems utilized for collecting, disseminating or storing information used in the issuance of REAL ID licenses.”²⁰² This comprehensive security plan must also include “how the State will protect the privacy of the data collected, used, and maintained in connection with REAL ID, including all the source documents.”²⁰³ The certification packages must also include an exceptions process for people who cannot fulfill the requirements necessary to receive a REAL ID card.²⁰⁴

The two-year delay in releasing draft regulations and the short timeline for the States to create “certification packages” detailing how they will comply with the final regulations makes it virtually impossible for the States to create useful implementation plans that take privacy and security questions into consideration. This fast-track scheduling makes it appear dubious that DHS will take comments submitted by the public into account when creating the final regulations for REAL ID implementation, though the agency is required to under law.

XIV. REAL ID MUST BE REPEALED

REAL ID is fundamentally flawed because it creates a national identification system. It cannot be fixed no matter what the implementation regulations say. Therefore,

²⁰¹ REAL ID Draft Regulations at 10,824, *supra* note 1.

²⁰² *Id.* at 10,825.

²⁰³ *Id.* at 10,825.

²⁰⁴ *Id.* at 10,822.

the REAL ID Act must be repealed. Federal legislation has been introduced to repeal the REAL ID Act.²⁰⁵ Arkansas, Maine, Idaho, Montana, and Washington State all have passed legislation rejecting the REAL ID Act, and more than 20 other states are debating similar legislation.²⁰⁶

The Department of Homeland Security protests that it must implement the REAL ID Act, but Homeland Security Secretary Michael Chertoff has worked with members of Congress in the past on problems with implementing the REAL ID Act.²⁰⁷ He can continue to work with members of Congress to reject this national identification scheme.

XV. CONCLUSION

For the foregoing reasons, the Coalition urges the Department of Homeland Security to recommend to Congress that REAL ID is unworkable and must be repealed. The REAL ID Act creates an illegal *de facto* national identification system filled with threats to privacy, security and civil liberties and undermines well-established principles of law found in the Privacy Act. Assuming that REAL ID is repealed, any subsequent legislation should be subjected to extensive review that explicitly addresses all of the issues raised in this document.

Respectfully submitted,

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

²⁰⁵ See EPIC's page on National ID Cards and the REAL ID Act page, http://www.epic.org/privacy/id_cards/ (information about federal and state legislation concerning REAL ID).

²⁰⁶ *Id.*

²⁰⁷ At the press conference announcing the release of the draft regulations for REAL ID implementation, Secretary Chertoff said, "And, I want to say in particular that in formulating the proposal that we're announcing today we were delighted to work closely with governors and members of Congress." Michael Chertoff, Sec'y, Dep't of Homeland Sec., Remarks at a Press Conference on REAL ID (Mar. 1, 2007), transcript available at http://www.dhs.gov/xnews/releases/pr_1172834392961.shtm.

AND

[EXPERTS IN PRIVACY AND TECHNOLOGY]

STEVEN AFTERGOOD, FEDERATION OF AMERICAN SCIENTISTS*
 PROF. ANITA ALLEN, UNIVERSITY OF PENNSYLVANIA LAW SCHOOL
 PROF. ANN BARTOW, UNIVERSITY OF SOUTH CAROLINA SCHOOL
 OF LAW
 PROF. CHRISTINE L. BORGMAN, UCLA DEPARTMENT OF
 INFORMATION STUDIES
 PROF. JAMES BOYLE, DUKE LAW SCHOOL
 DAVID CHAUM
 PROF. JULIE E. COHEN, GEORGETOWN UNIVERSITY LAW CENTER
 SIMON DAVIES, PRIVACY INTERNATIONAL
 WHITFIELD DIFFIE, SUN MICROSYSTEMS
 PROF. DAVID FARBER, UNIVERSITY OF PENNSYLVANIA DEPARTMENT
 OF COMPUTER AND INFORMATION SCIENCE
 PHILIP FRIEDMAN
 DEBORAH HURLEY
 PROF. JERRY KANG, UCLA LAW SCHOOL
 CHRIS LARSEN, PROSPER
 PROF. GARY MARX, MASSACHUSETTS INSTITUTE OF TECHNOLOGY
 MARY MINOW, LIBRARYLAW.COM
 DR. PETER G. NEUMANN, SRI INTERNATIONAL
 DR. DEBORAH PEEL, PATIENT PRIVACY RIGHTS
 STEPHANIE PERRIN, SERVICE CANADA
 PROF. ANITA RAMASASTRY, UNIVERSITY OF WASHINGTON
 LAW SCHOOL
 BRUCE SCHNEIER, BT COUNTERPANE
 ROBERT ELLIS SMITH, PRIVACY JOURNAL
 PROF. DANIEL J. SOLOVE, GEORGE WASHINGTON UNIVERSITY
 LAW SCHOOL
 PROF. FRANK M. TUEKHEIMER, UNIVERSITY OF WISCONSIN
 LAW SCHOOL, MADISON

* affiliations are only for identification purposes



Testimony of Allen Gilbert

Executive Director

American Civil Liberties Union of Vermont

On the topic of

Will REAL ID Actually Make Us Safer?

An Examination of Privacy and Civil Liberties Concerns

U.S. Senate Committee on the Judiciary

May 8, 2007, 10 a.m.

Dirksen Senate Office Building, Room 226

American Civil Liberties Union of Vermont, 137 Elm St., Montpelier, VT 05602



Will REAL ID Actually Make Us Safer?

An Examination of Privacy and Civil Liberties Concerns

Testimony by Allen Gilbert, executive director, ACLU-Vermont

Submitted to the U.S. Senate Committee on the Judiciary, May 8, 2007

1. Oral testimony given before the Committee

2. Appendices

Appendix A – ACLU Real ID Scorecard

Appendix B – Status of Anti-Real ID Legislation in the States (map)

Appendix C – Vermont news articles about Real ID

C.1. “National ID System Expensive, Complicated,” editorial from *Burlington (Vt.) Free Press*, Aug. 27, 2006

C.2. “Federal Legislation – Real ID Act of 2005,” from *Vermont Privacy News*, Summer 2005

C.3. “National ID Law Could Mean Problems for State,” from *Rutland (Vt.) Herald* and Barre-Montpelier (Vt.) *Times Argus*, Jan. 14, 2006

C.4. “Identity Guidelines Could Cost State \$8 Million,” from *Rutland (Vt.) Herald* and Barre-Montpelier (Vt.) *Times Argus*, May 3, 2007

Testimony by Allen Gilbert, executive director, ACLU-Vermont

U.S. Senate Committee on the Judiciary, May 8, 2007

My name is Allen Gilbert. I live in Worcester, Vermont. I've been a journalist, a teacher, and I ran a small business for 15 years. I'm currently the executive director of the American Civil Liberties Union of Vermont.

Thank you, Chairman Leahy, and Committee Members for this invitation to testify.

People in Vermont have a lot of unanswered questions about Real ID. Seldom have I encountered an issue that raises concerns among such a wide range of people.

I can talk with a legislator about Real ID, and she'll point out that the National Conference of State Legislatures expresses misgivings about the program.

I can talk with a member of the National Gun Owners, and he'll worry about government intrusion.

A member of an advocacy group for victims of domestic and sexual violence worries that Real ID threatens protection programs for women and children.

The Ancient Order of Hibernians doesn't like Real ID, and neither does the American Friends Service Committee.

Earlier this year, the Government Operations Committee of the Vermont House of Representatives passed, unanimously, a resolution opposing Real ID. The resolution was subsequently approved, also unanimously, by the full House. The longest-serving member in the Vermont House sits on the Government Operations committee. Rep. Cola Hudson was born when a fellow Vermont Republican, Calvin Coolidge, was president. Rep. Hudson just shook his head "no" when Real ID was described.

Our Motor Vehicles commissioner testified in another committee about the "re-enrollment process" required by Real ID. Everyone will have to visit a DMV office with proper documents. For some people in Vermont, that means a long trip. And when they get to the DMV office, our commissioner said, "The jokes about waiting in line at DMV are no longer going to be jokes but reality."

Long-time residents will feel like suspects when they're required to report and show their papers. Our commissioner noted that her father is 82 years old. He's had a driver's license for years. It's going to be hard to tell him, she said, that he has to prove his identity before he can get his license renewed. People in Vermont pride themselves on

being part of tightly knit communities. Questioning who someone is, is seen as a sign of unfriendliness.

Birth records are kept by town clerks in Vermont. The clerks -- some of whom work part-time -- are already in a frenzy over the thought of complying with the myriad requests for records that they'll get because of Real ID.

A state senator who in his other life runs a construction company and races stock cars, said, "I'm not sure if it's the budgetary concern or the privacy concern or the nightmare it's going to create that concerns me most about this."

A series of data breaches this winter in Vermont led people to wonder about the security of stored data anywhere. DMV officials acknowledge that there are hundreds of unauthorized attempts daily to get at the department's information database.

Increasingly, Vermonters are worried that too much data is being collected about too many things. It's not just a sense that privacy is eroding. Vermonters are worried that their identities will be stolen by identity thieves.

Vermonters are pretty responsible people. They generally step up to the plate when asked to do the right thing. But many people aren't so sure that Real ID is the right thing. It seems too big, too expensive, and too centralized. Real ID has hit a nerve with people.

Mr. Bruce Schneier will testify later this morning. I've heard him lecture, and one thing that he's said has really stuck with me. He has said that security is an equation, with one side being what you're giving up and the other side what you're getting in return. I'm afraid that with Real ID, we're giving up too much and not getting much, if anything, in return.

Real ID is also going to cost the states a lot of money. The cost in Vermont is now estimated at around \$8 million. That is a substantial expenditure for us. Some of our state senators want to raise license fees and call the increase a congressional Real ID tax.

The cost, the implementation, the risk of identity theft -- these things worry Vermonters. Vermonters are not convinced that Real ID is a program that will make Americans safer. It is a caution that I hope Congress will heed.

People are saying that we need minimum licensing standards, and we agree. That's why the ACLU participated in the negotiated rulemaking created by the Intelligence Reform and Terrorism Prevention Act of 2004. If Rep. Sensenbrenner hadn't interfered, we would have had those standards by September 2005 and they would have been created in a cooperative fashion. But, what Janice Kephart and Jim Carafano are proposing is to push forward with a system that the states are rejecting en masse and that -- because of its impracticality, extraordinary costs, and constitutional infirmities -- will be delayed years and years, if it's ever built at all.

There's a better way. On behalf of the ACLU, its 53 affiliates and hundreds of thousands of members nationwide, I urge you to mark up and move S. 717, the Akaka-Sununu-Leahy-Tester bill. That bill would replace Real ID with sensible, cost-effective driver's license standards. The problems with Real ID would be fixed, and the standards could be achieved in a cooperative fashion with state officials, federal government agencies, and privacy and civil liberties experts. S. 717 paves the way for a better system, one that complies with the 9/11 Commission's minimal statement.

And S. 717 will not threaten to change the quality of life of Vermonters, in all the ways that Real ID will.

The written testimony I am submitting includes the ACLU's comments on the rules proposed by Homeland Security to implement Real ID, a map showing state-by-state actions regarding Real ID, and Vermont news articles on Real ID.

Again, thank you for this opportunity to testify before you.

Appendix A

ACLU Real ID Scorecard



New Federal Regulations Get an 'F' in Addressing Issues with the Real ID Act

DHS Rules Score Only 9 Percent On ACLU Scorecard

On March 1st, the Department of Homeland Security issued proposed Federal regulations for implementing the Real ID Act, the law that would federalize state driver's licenses and the motor vehicles departments that issue them and create the nation's first-ever de facto national identity card system.

In preparation for the issuance of the regulations, the ACLU prepared this Real ID Scorecard to assist in the systematic analysis of this complex legislation. It attempts to list all the issues that have been identified as concerns with Real ID by a variety of parties, including privacy activists, domestic violence victims, anti-government conservatives, religious leaders, and DMV administrators.

The Scorecard shows that the regulations utterly fail to remedy the problems with Real ID. Of the 56 issues listed, the regulations passed 5 (9 percent), scored an incomplete on 9 (16 percent), and failed the rest.

Indeed, the government was often strikingly forthright in admitting that the regulations do not solve deep problems with this statute. The regulations acknowledge that wait times at the DMV will increase substantially; that many applicants will not have source documents they need to obtain a Real ID card; that "there is no single way for States to comply" with Real ID's verification requirements by the statute's deadline "or in the reasonably foreseeable future"; and that the regulations will be extremely costly. (The most authoritative prior estimate of Real ID's costs was \$11 billion. The regulations, however, concede that the price tag for Real ID will come to a whopping \$23 billion.)

DHS cannot be blamed for such problems when they arise out of what is, at its core, simply an ill-conceived and impossible law. In other cases, however, the government fails to set forth rules that could have solved or ameliorated problems with the act. On Real ID's onerous verification requirements, for example, DHS did not ease burdens on states and individuals, but in fact increased them (by requiring verification of all identity documents not just to obtain a Real ID, but even to renew one; requiring not one, but two documents showing proof of address). Similarly, the agency acknowledges the danger of license data being scanned by third parties, but fails to take action to stop the problem, and merely encourages the states to come up with a solution. DHS says it "leans toward" requiring that data to be encrypted but opts not to due to "practical concerns."

Aside from failing to solve the problems with Real ID, the regulations add up to a striking federal takeover of state DMV offices. The regulations put the federal government in the position of dictating the minutiae of DMV operations, from the colors that can be used on a license to the computer format in which image files (.JPG) and scanned documents (.TIF) are stored, to the details of how a DMV office secures its plant, to many other details.

Initial media coverage of the new regulations focused on the additional time that states were being given to comply with Real ID. But what this scorecard makes clear is that Real ID is a fundamentally misguided policy that will waste large amounts of money and other limited resources, and impose significant inconveniences, without improving our safety. We don't need to delay Real ID, we need to throw it away and start fresh.

The grades

The following grades indicate whether the federal regulations succeed in fixing each problem. In cases where DHS addressed the problem but could not or did not fix it, we list a grade of "incomplete."

Problems with the act have been grouped into four categories: 1) impact on individuals, 2) impact on privacy, 3) impact on states and 4) impact on Constitutional rights. Page numbers refer to pages in the Federal Register notice.

Impact on Individuals		
PASS	FAIL	INC
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Increased wait time at the Department of Motor Vehicles (“DMV”). Many state DMVs predict extensive increases in customer wait times resulting from the many new requirements imposed by Real ID. In a survey by the American Association of Motor Vehicle Administrators (AAMVA), states predict that Real ID will bring increased “customer traffic flow and customer wait/visit time in all field offices” and will have a “significant influence on customer service.” (<i>The Motor Vehicle Administrators Survey on Real ID: An ACLU White Paper</i>) The regulations impose significant new burdens on individuals that, as DHS acknowledges (p. 10,843, Federal Register, Volume 72, Number 46), will increase wait times and service times at DMVs, as well as the time necessary to obtain new source documents. Partly this would be caused by the fact that initial applications for all Real IDs (as well as many renewals) must be done in person (p. 10,854), and many applicants will not have source documents when they need them (p. 10,845). DHS estimates opportunity costs to individuals from waiting at the DMV at \$1.7 billion (p. 10,845).</p>		
PASS	FAIL	INC
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>“Full Legal Name” requirement. Wide inconsistency often exists between names even on federal documents, such as a social security card and a passport belonging to the same individual. All these records must be verified and harmonized under REAL ID prior to the issuance of a license. Recently in Alabama tens of thousands of older drivers had difficulty renewing licenses because the names in their DMV records were not consistent with other records such as the Social Security database. Many Americans have records that reflect not only their “legal name”, but also the everyday names they use. James Joseph Johnson Jr. may have documents in the name of Jim Johnson, JJ Johnson, Jim Johnson Jr., Joe Johnson, etc. (<i>ACLU analysis, “The Alabama Mess: One State Tries to Begin Tackling Real ID”</i>). The regulations do not address or solve the problem of individuals who are recorded under different names on different documents or in different databases. The regulations simply state that all license holders must use their legal name in applications and that the identity documents they submit must contain that name (p. 10,853).</p>		

PASS <input type="checkbox"/> FAIL <input checked="" type="checkbox"/> INC <input type="checkbox"/>	<p>Individuals with changed names. Individuals whose name on one source document does not match the name on another will find themselves in a bureaucratic bind under Real ID. This is a substantial portion of the population including women who have taken their spouses' last names and a large percentage of the Asian-American community (whose first and last name may be switched on their source documents). (<i>National Governors Association ("NGA")</i>, <i>National Conference of State Legislators ("NCSL")</i>, & <i>AAMVA, "The Real ID Act: National Impact Analysis"</i>) According to the regulations, in order to prove a name change an applicant must present a certified copy of a record from "US or state-level Court or government agency" (pp. 10,835 & 10,851). This does not address the issue of individuals whose name is recorded differently in different databases or records. It also requires individuals to take the formal step of changing their name; currently in many states it is lawful to simply use a different name as long as an individual has no fraudulent intent. Finally, many marriage certificates are issued by county (not state) officials, making it unclear how individuals could comply.</p>
PASS <input type="checkbox"/> FAIL <input type="checkbox"/> INC <input checked="" type="checkbox"/>	<p>Principal address requirement. The act requires, without exception, that compliant IDs contain one's "principal address." It is unclear how people without such an address or who live in different places – such as students, those who live in RVs and other mobile homes, and the homeless – will solve this issue. (<i>See ACLU, "Real Costs: Assessing the Financial Impact of the Real ID Act on the States"</i>) The regulations attempt to address this issue by defining principal address as the place where an individual has his "true, fixed and principal home" (p. 10,851), and stating that DMVs can make exemptions for the homeless (pp. 10,803 & 10,836). There is still some concern regarding whether all states will be able and willing to create workable methods for utilizing these exemptions.</p>

PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Threat to safety from principal address requirement. A number of states have laws that allow judges, police officers, domestic violence victims, or others at risk of retaliatory criminal violence to use agency addresses or P.O. boxes in lieu of their actual residence address. Yet states cannot keep those laws on the books if they are to comply with Real ID. (<i>"Motor Vehicle Administrators Survey"</i>) Under the regulations, the vulnerability of domestic violent victims and others will be increased. The regulations do create a partial exemption to the principal address requirement, but it is inadequate. It covers "individuals who are entitled to enroll in State address confidentiality programs, whose addresses are entitled to be suppressed under State or Federal law or by a court order" and some individuals protected by immigration law (p. 10,836). However, only 24 states currently have such confidentiality programs, according to the National Network to End Domestic Violence. In the other jurisdictions, victims are now protected instead by the fact that they are not required to put their principal address on their license – as are federal judges, who are not shielded by state laws at all (DHS solicits comments on how to fix the problem with regard to the judges). The regulations seem to maintain the same status that police officers, state and local judges, and protected witnesses currently enjoy under state law. However, by removing the option of not listing an address and relying solely on state laws that don't cover many vulnerable individuals, the regulations fail badly.</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Disproportionate burden on low-income individuals. It is feared poorer people will find it harder not only to absorb higher license-issuance or renewal fees, but also to skip what will sometimes be multiple days of work in order to stand in long queues to prove their identities in order to obtain a Real ID. (<i>ACLU, "Real Answers: FAQ on Real ID"</i>) Real ID is expected to cost \$23.1 billion nationally (p. 10,845), including \$7.8 billion in costs to individuals, and will require increased time waiting at the DMV and seeking source documents. The regulations estimate that visits to the DMV alone will cost Americans \$1.7 billion.</p>
PASS FAIL INC <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<p>Individuals who lack birth certificates. Over time, many records are lost through natural disasters, such as flood or fire, and by human error. And the births of many, especially older citizens from rural areas, simply were not recorded. Because the birth certificate is likely to be one of the core documents that must be verified (especially to prove citizenship) it is not clear how these problems will be addressed. (<i>"FAQ"</i>) The regulations seem to address this issue by allowing states to create an exemption process for individuals who do not have a birth certificate (p. 10,830 and 10,852). (Ironically, this exemption would seem to undercut the entire security rationale for Real ID: that identity can only be proved by presenting other "breeder documents" like birth certificates).</p>

PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Foreign-born lawful residents who lack passports. The only foreign document that is acceptable to DMVs under Real ID is an official passport. But that doesn't meet the needs of many legal immigrants, including refugees and dissidents or others who may face hostility or a lack of cooperation from their home governments in obtaining the required documents. (<i>"FAQ"</i>) DHS attempts to address this problem by allowing for the acceptance of some foreign documents other than passports. But there are some categories of immigrants who, while legal, will still not possess any of the documents listed by DHS (for example, asylum seekers).</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Same-day licenses. State DMV officials report that Real ID could largely prevent over-the-counter issuance of some or all IDs, resulting in shifts from relatively instant issuance to having to mail documents to applicants, and an overall process that could range from 2 to 6 weeks pending approval of verified documents. (<i>"Motor Vehicle Administrators Survey"</i>) While in theory, if every verification database existed and was fully operational, applicants could have their documents verified instantly and walk away with a Real ID, the regulations make it clear that that simply is not going to happen, at least in the foreseeable future. There are too many burdens in the regulations, too many documents to be verified, and too few existing systems through which to do that, for there to be any realistic chance that same-day licenses will continue to be possible.</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Fewer offices. DMV officials in some states also report that the cost increases driven by the act's requirement may force them to close some itinerant field stations and eliminate mobile offices, which can impose considerable burdens on citizens of rural, low-density states. (<i>"Motor Vehicle Administrators Survey"</i>) The regulations fail this test because they create extensive security requirements for DMV offices (p. 10,855), making it unlikely that many small DMV offices will be able to remain open at a cost the states can afford. This would inconvenience consumers by forcing smaller offices to close their doors and have a disproportionate impact on Americans who live in rural communities.</p>

PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Internet or mail transactions. Because of the verification requirements, DMV officials report that Real ID could reduce or end mail and Internet address changes and renewals, further straining the resources of DMVs and imposing burdens on drivers and other applicants. (<i>"Motor Vehicle Administrators Survey"</i>) Issuing of licenses through the Internet and mail will not be possible for at least the first 5 years under Real ID because every individual will be required to register in person to get a Real ID. Remote renewals of a Real ID (after initial issuance) will only be possible for every other renewal, and only if none of the licensing information (such as address) has changed (p. 146). Also, it is unclear whether the regulations will allow the mailing of licenses or whether license holders will have to return to the DMV to receive a license.</p>
PASS FAIL INC <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<p>Change of address. Currently individuals simply notify their DMV when they move. However, the principal address requirement of Real ID (see above) may require people to re-register with the DMV in person every time they change addresses so that their new address can be verified and they can be issued a new ID card. This will not only impose substantial inconveniences on individuals, but also raise costs for DMVs. (<i>NCSL et al, "Impact Analysis"</i>) The regulations seem to address this issue by implying (though not stating directly) that an individual will only have to change their address information when renewing their license (p. 10,845).</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Disruption in driving caused by verification procedures. Will states be able to issue an interim driver's license for individuals whose source documents cannot be immediately verified or will these individuals be prevented from driving? Will such a temporary ID be acceptable for air travel? The regulations make no provision for this type of temporary license and fail to take into account the fact that delays in verification (due to such inevitabilities as computer problems or verification delays) will make it increasingly difficult to perform same-day licensing.</p>
Impact on Privacy	

PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>National ID. Privacy advocates fear the Real ID and its national database will become a national identity registry. The act states that Real IDs shall be required not only for activities like boarding aircraft, but also for “any other purposes that the Secretary [of Homeland Security] shall determine.” This provision allows the Department of Homeland Security to expand unilaterally the scope of identity requirements creating the real possibility of mission creep. Some groups have already suggested that Real ID should become a voter registration card and a border crossing document. (“FAQ”) The regulations do nothing to prevent Real ID from becoming a de facto National ID card. They create a vast infrastructure for such a system, including a common machine readable element (with no protection against private-sector exploitation) and the construction of a national interlinked database. The regulations already require the card in order to fly or enter a federal facility, and explicitly state that Real ID will be considered for a number of other functions including receiving a passport, military common access card, and transportation worker identification card (p. 10,823).</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Private-sector piggybacking. The “common machine-readable technology” on Real IDs would allow for easy, computerized transfer of the data on the cards not only to the government but also to private parties. Already, many bars and clubs collect all their customers’ information by swiping driver’s licenses handed over to prove legal drinking age. There is concern that even if the states and federal government successfully protect the data, machine readability will result in a parallel, for-profit database on Americans, free from the limited privacy rules in effect for the government. (“FAQ”) The regulations do not protect individuals from private sector piggybacking. They state that protecting machine readable technology from private sector access is outside the scope of DHS responsibility and leave such regulation to individual states (p. 10,837). They decline to require that data on the card be encrypted, leaving it open to reading by a private-sector entity.</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>A single interlinked database. Will the national database be secure from identity thieves and criminals? Advocates argue that the government’s poor record at information security and at preventing insider fraud and abuse may mean Americans are less secure as a single national database makes their information more vulnerable and available from more sources. (<i>Center for Democracy and Technology, “Unlicensed Fraud”</i>) The regulations fail on this issue because they require creation of a national database of interlinked state systems (p. 10,855). DHS denies there will be a national database, but having one central database in Washington or 50 state databases in the individual states, all linked together with identical comments and an identical form, are effectively the same thing. Moreover the regulations explicitly provide that the Department is “committed to the expedited development and deployment of a common [federated] querying service” (p. 10,825).</p>

PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Insider fraud. Advocates have also argued that linking databases will give more and more parties “legitimate” access to the data and that information that can be accessed by multiple disparate parties is a recipe for fraud. Fraud by DMV officials is a major cause of identity theft. Insider fraud is one of the core problems with Real ID. It is not solved in the regulations nor is it clear that there is a solution to the problem as the act is written. The regulations attempt to address this issue by requiring criminal background and credit checks for employees (p. 10,856), but it is unclear whether or how much such checks would reduce fraud by the many insiders who do not have a troubled record. Such fraud is almost certain to continue, especially in light of the fact that the perceived authenticity of a Real ID license is likely to make it even more valuable on the black market and create a new wave of insider fraud. (For more information on identity theft and Real ID please see comments by the Privacy Rights Clearinghouse available here: http://www.privacyrights.org/ar/real_id_act.htm)</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Accountability vacuum. Security experts note that a system is only as secure as its weakest point. There is no mechanism to guarantee that every DMV follows adequate procedures and the linked distributed system makes accountability extremely difficult to enforce. Further, a single breach at a single DMV could compromise the entire system and expose the data of every American who drives. A state that finds its citizens’ data threatened or stolen due to the negligent practices of another state will have no remedy or recourse under the regulations. While securing private information is vital, the regulations provide no guidance as to how states should do so, or what a state can do if other states’ efforts fall short. (p. 10,855). The regulations state that information sharing between states will be a state function with only limited oversight from DHS (pp. 10,825).</p>
PASS FAIL INC <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<p>Protecting source documents. Real ID requires all source documents for licenses to be retained either electronically or in storage at the DMV. Protecting these valuable document troves from security breaches will require the devotion of significant resources to new computer hardware and software, systems redesign, security consulting, and staff expansions. It is expected that identity thieves will quickly recognize that the DMV’s records are a central location for obtaining all the documents they need to commit fraud. (“<i>Real Costs</i>”) The regulations state that securing private databases must be part of state physical security measures, but provide no guidance as to how states will secure this information (p. 10,855).</p>

PASS <input type="checkbox"/> FAIL <input checked="" type="checkbox"/> INC <input type="checkbox"/>	<p>Effect on state privacy laws. States have varied privacy and safety laws governing everything from what information can be collected for the purpose of driver's licensing, to what information can be contained on the machine-readable component of an ID card. It is expected that Real ID will force state legislatures to alter or repeal many of these laws – potentially creating new privacy and security problems. (See <i>"The Impact of Real ID on Current State Laws,"</i> and accompanying chart prepared by Stanford University Law School) The regulations allow states to impose greater privacy protections than required by regulation and allow some flexibility to protect the confidentiality of address information (p. 10,854). But they are silent on how state laws that are directly in conflict with the Real ID regulations will be affected (p. 10,849). For example, in order to protect against identity theft, California law allows the DMV to destroy all records that are no longer necessary to issue a license. In New Hampshire, the wholesale sharing of motor vehicle information with other states is prohibited and sharing shall only be "on a case to case basis." Such state laws would have to be changed in order to secure Real ID compliance (p. 10,857).</p>
<p>Impact on the States</p>	
PASS <input type="checkbox"/> FAIL <input checked="" type="checkbox"/> INC <input type="checkbox"/>	<p>Unfunded mandate. Real ID requires sweeping changes to state driver's licenses and the systems by which those licenses are administered. A partial cost estimate issued jointly by AAMVA, NGA, and the NCSL estimated the cost of Real ID on the states at \$11 billion. Congress has currently appropriated \$40 million to offset Real ID costs. (NCSL <i>et al</i>, <i>"Impact Analysis"</i>) The regulations acknowledge that the AAMVA-NGA-NCSL estimate is inadequate and that the actual cost of Real ID will be \$23.1 billion (p. 10,845).</p>

<div>PASS FAIL INC</div> <div><input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/></div>	<p>Effect on DMVs of standardizing data elements. Real ID imposes a requirement for uniform data elements on state IDs. Standardizing these elements will vary in difficulty from state to state, but in many cases will require the reprogramming of multiple interlocking state databases, computer entry screens, communications protocols, and paper forms. (<i>ACLU analysis, "Real Burdens: the Administrative Problems REAL ID Imposes On The States"</i>) The regulations require states to share all their driver's license information. This will force states to make costly changes to their Information Technology (IT) systems. The regulations provide no guidance on how such changes are to be effected, and place the entire burden of constructing a data-sharing system on the states (pp. 10,825 & 10,855). The regulations also impose additional onerous IT requirements, such as requiring states to retain the photographs of all applicants (not just license holders) (p. 10,851) and retaining all name information on applicants even if they subsequently change their name (pp. 10,835 & 10,851).</p>
<div>PASS FAIL INC</div> <div><input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/></div>	<p>Effect on recent improvements to state IT systems. The NCSL reports that 21 states have invested \$289 million over the last five year to modernize their DMV information systems. Real ID may force much of this work to be thrown out. (<i>NCSL et al, "Impact Analysis"</i>) Because the regulations do not provide guidance regarding how data sharing will be implemented, it is unclear to what degree states will be able to rely on their previous (costly) IT system overhauls (pp. 10,825 & 10,855).</p>
<div>PASS FAIL INC</div> <div><input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/></div>	<p>Cost of processing new applicants. Real ID's requirement that it be used for a host of federal purposes may force millions of Americans to sign up for driver's licenses or ID cards. This would result in an unplanned wave of new applicants swamping DMVs. The regulations assume that there are 240 million licensees. This number seems to encompass most of the ID holders in the US.</p>
<div>PASS FAIL INC</div> <div><input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/></div>	<p>DMVs will have to reprocess existing licensees. The document verification process will also have to be completed for the entire population of people (approximately 200 million) who already have current licenses and IDs. Motor vehicle administrators have complained that this will significantly strain DMV resources. (<i>"Real Burdens"</i>) Because the regulations state that all license holders will have to reply in person to receive a Real ID-compliant license (p. 10,854), DMVs will not be able to take advantage of the ease of processing licenses over the Internet or through the mail. This change will substantially increase the number of people coming to DMVs and significant strain existing resources.</p>

PASS <input type="checkbox"/> FAIL <input checked="" type="checkbox"/> INC <input type="checkbox"/>	<p>Diversity in licensing systems. States have chosen a variety of methods for issuing licenses. In Kentucky, for example, licenses are handled by court clerk offices, in Alabama by probate judges, in Nebraska by county treasurers, and in Oklahoma by third party vendors. It is unclear whether Real ID regulations will continue to allow states to operate under these different licensing models. (<i>"Motor Vehicle Administrators Survey"</i>) The regulations do not address these issues, and taken as a whole the regulations make it clear that many states will have to drastically alter their licensing schemes.</p>
PASS <input type="checkbox"/> FAIL <input checked="" type="checkbox"/> INC <input type="checkbox"/>	<p>Appeal process. Mistakes in existing DMV and other databases may result in delays or even inability to get a drivers' license. In light of this high penalty some type of appeal process will have to be created to deal with mistakes and document errors. The regulations contain no appeals process for individuals who are the victims of errors in the information used to verify their identity. Instead, individuals will have to correct errors with the database owners (pp. 10,833 & 10,852). (States, however, can appeal determinations made by DHS that their systems are not Real ID compliant [p. 10,857].)</p>
PASS <input type="checkbox"/> FAIL <input checked="" type="checkbox"/> INC <input type="checkbox"/>	<p>Expertise in immigration law. The act bars states from issuing compliant IDs to any non-citizen who cannot prove their identity and present verified documentary evidence that they are covered by one of an enumerated number of lawful immigration statuses. But the complexity of our immigration laws make it likely that identifying and processing a variety of different immigration documents will be a difficult task. (<i>"FAQ"</i>) The regulations require intimate familiarity with multiple immigration documents in order to issue a Real ID in two contexts. First, DMV employees have to be trained to recognize a number of types of fraudulent documents for proof of citizenship (visa, permanent resident card, EAD, Certificate of Citizenship, or Certificate of Naturalization). Second, DMV employees will have recognize the very obscure immigration documents that prove that an individual is not eligible for a Social Security number (those that prove an alien "is currently in a non-work authorized non-immigrant status") (pg. 10,829).</p>
PASS <input type="checkbox"/> FAIL <input checked="" type="checkbox"/> INC <input type="checkbox"/>	<p>Lawful status not described in the Act. Immigration advocates have complained that there are a number of ways that an immigrant can be in the country lawfully that are not described in the act. It is not clear if these individuals can qualify for a Real ID. Because the regulations do not expand the description of lawful status for purposes of obtaining a Real ID beyond statutory guidelines, numerous individuals, such as asylum seekers, cannot get any type of Real ID, even though they are in the country lawfully.</p>

PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	“Full Legal Name” particularly onerous. The Act requires that compliant identity papers contain individuals’ full legal names. However because a portion of the population possesses extremely long names, the name for licenses is recommended to be at least 100 (some say 126) characters long. For many states this would mean redesign of their entire database structures and program interfaces to standardize how information is entered in each field office and how it is stored centrally. They will also have to revise information and application forms, and train staff to verify legal name. (<i>“Real Costs”</i>) The regulations require states to retain 39 characters of an individual’s legal name for the front of a license and 125 characters for the machine readable zone (MRZ) of the license, placing a new burden on the states by requiring them to modify their systems to collect this information in two different ways in order to secure it in their databases and place it in the MRZ (pp. 10,835, 10,853 & 10,854).
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	“Full legal name” requirement reaches beyond DMVs. Legal name changes in DMV systems will impact other, linked systems such as CDLIS (a commercial license database) and PDPS (a problem driver database) as well as serving as the access point for other systems, including law enforcement, insurance companies, and the election registry. (<i>“Real Costs”</i>) The regulations provide no guidance on how states are to reconstruct their information systems (p. 10,855).
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Limited real estate on physical cards. Many states may have to redesign the face of their ID cards – where space is already limited – to include longer names and new data elements such as principal address. (<i>“Real Costs”</i>) The regulations do not provide any flexibility regarding the information to be placed on the front of the card (p. 10,853).
PASS FAIL INC <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	License holders with multiple addresses. If mailing address and principal address differ, states will have to retain both – one for printing on the license and one for correspondence. Some individuals – such as students and those who own multiple homes – reside in more than one state. Regulations address this issue by assuming individuals will choose one principal address, which will be the place where they maintain their “true, fixed and permanent home” (p. 10,851).

<p>PASS FAIL INC</p> <p><input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/></p>	<p>Creation of interconnected database. Real ID requires that each state provide all other states with electronic access to the information contained in its motor vehicle database. Because state DMVs each have their own IT systems with different level of capability and interoperability DMV officials believe this will be an extraordinarily difficult task. (<i>"Motor Vehicle Administrators Survey"</i>) The regulations require a national database of interlinked state systems both for ascertaining whether an individual has a license in another state and for sharing motor vehicle information (p. 149). The regulations provide no guidance on how states are to share information, and place the entire burden constructing a data sharing system on the states (pp. 27 & 149). Nor do they mitigate any of the requirements that states standardize information in their IT systems.</p>
<p>PASS FAIL INC</p> <p><input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/></p>	<p>Cost of data sharing. A system similar to that mandated by Real ID, the commercial driver's license pointer system (CDLIS), which covers truck drivers and other commercial drivers, costs roughly \$0.08 per month/per record, according to the AAMVA. At the same cost, the price for covering the roughly 200 million current US license holders under Real ID would be \$192 million per year. However, since the Real ID database will include significantly more information than CDLIS, this figure would likely be much higher and it is unclear how this cost burden would be met (and by whom). (<i>"Real Costs"</i>) The regulations indicate that data sharing is likely to be costly. DHS estimates the total for information sharing and IT services to be \$1.4 billion. The regulations note that states already use information systems like CDLIS and indicate that it may provide a model for information sharing (p. 10,825), but provide no guidance for implementing Real ID's much more substantial information-sharing requirements (p. 10,855).</p>
<p>PASS FAIL INC</p> <p><input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/></p>	<p>Document verification. The Real ID Act includes a requirement that states "shall verify, with the issuing agency, the issuance, validity, and completeness of each document required to be presented" to get a Real ID card. No electronic system or systems currently exist which is capable of performing this task. Particular concerns exists regarding birth certificates because they are issued by over 6,000 separate jurisdictions within the United States and there is no central database of certificates (<i>"Motor Vehicle Administrators Survey"</i>) It is impossible to evaluate whether the regulations solve the problem of document verification because most of the verification databases are in their infancy, and because databases will never exist for verifying address (pp. 10,831). The states are required to find their own methods for verifying documents until electronic databases exist (p. 10,831).</p>

PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Inadequacies in existing verification systems. An additional verification problem is that DMVs report that existing database such as SAVE (for verifying immigration status) would be inadequate for Real ID purposes either because they are expensive, inaccurate, or do not provide a timely response. (<i>"Motor Vehicle Administrators Survey"</i>) The regulations fail to address this issue except in a cursory fashion. The fact is that many verification databases that do exist (such as SAVE and SSOLV) are incomplete, inaccurate and so far unable to perform the functions required by Real ID (pg 10,832).
PASS FAIL INC <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Verification cannot be compelled. The act requires DMVs to authenticate source documents with issuing entities (such as address checks from public utility companies). Because that process will impose substantial burdens on verifying entities it may be met with resistance. However state DMVS have no power to compel or reward compliance. The regulations circumvent this problem by stating that, in direct contradiction to the statute, DMVs won't have to verify addresses with the issuing agency. ("The proposed regulation would require States to establish a written policy identifying acceptable documents and how, or if, they will be independently validated or verified." [p. 10,831]). However, they still require documents like birth certificates to be verified even though there is no existing database of birth certificates from all 50 states.
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Investigations into Social Security Numbers. States are required to verify that an individual has a valid social security number – and requires that "[i]n the event that a social security account number is already registered to or associated with another person . . . the State shall resolve the discrepancy and take appropriate action." However it is not clear what "appropriate action" entails nor do state officials have the authority to change the Social Security database. (<i>"Real Burdens," "Motor Vehicle Administrators Survey"</i>) The regulations do not provide any guidance for states on this issue, simply stating, "In the event of a non-match with SSA, a DMV must not issue a driver's license or identification card to an applicant until the information verifies with SSA's database." (p. 10,852)
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Document storage. The act requires storage of electronic copies of source documents for 10 years or paper copies for seven years. DMVs lack the equipment and storage space for document retention. DMVs report that this will have a major impact on their operations – requiring additional staff, new equipment, policy changes, training, the remodeling or redesign of offices, and computer software, development, and storage costs. (<i>"Real Costs," "Motor Vehicle Administrators Survey"</i>) The regulations affirm this requirement and estimate the cost of data systems and information technology at \$1.4 billion.

PASS FAIL INC <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Standardizing the machine-readable element. Many states have already deployed a variety of machine-readable technologies – such as bar codes and magnetic stripes – on the licenses they issue. Real ID's standardization mandates will impose substantial costs on the large number of states that will have to replace their existing machine-readable components. (<i>"Real Costs"</i>) The regulations require states to use a 2-D barcode compliant with PDF417 standard (p. 10,854). The regulations state that 45 states have 2-D barcodes, plus the District of Columbia (p. 10,837). It appears that all or most of those barcodes comply with the PDF417 standard. However, if a significant number of DMVs report that they will need to make expensive changes to the format of their bar codes, this may change to a "fail."
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Additional costs for standardization. Police departments will have to be equipped with new readers, at significant cost to taxpayers. During the five-year changeover to full 50-state Real ID compliance, numerous data storage systems and sets of readers will have to be maintained simultaneously. (<i>"Real Costs"</i>) The regulations provide no additional funding to offset this concern. They state that the AAMVA-approved barcode can be read by a standard 2-D barcode reader (p. 10,837), but do not address costs for states that must convert to new machine readable standards.
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	Facial image capture. The act appears to mandate that image capture must apply not to all license recipients, but to all <i>applicants</i> . This will require a new database for pending and failed applications, alterations to the licensing process to change the stage at which an image is captured, and increased personnel and equipment for additional image capture. (<i>"Real Costs"</i>) The regulations confirm that DMVs will face an increased IT burden because they have to save photo images for at least one year for all applicants (not just those that receive licenses), and for ten years for those denied licenses because they are suspected of fraud (pp. 10,835 & 10,851).
PASS FAIL INC <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	Facial recognition technology. The act's requirements for "facial image capture" may require states to purchase facial recognition technology and begin strictly regulating how photos are taken to correct for variations in lighting, expression, camera type, background, and the exposure of facial characteristics, such as facial hair, glasses, headscarves, etc. Facial recognition technology is often costly, inaccurate and difficult to implement. (<i>"Real Costs"</i>) The regulations do not fully address the issue of face recognition. While they take some steps consistent with the technology, such as prescribing the physical appearance of individuals in photos (p. 10,853-10,854), they are silent on whether photos will be used as part of a facial recognition system.

PASS <input checked="" type="checkbox"/> FAIL <input type="checkbox"/> INC <input type="checkbox"/>	<p>Security clearance. Real ID requires that state employees who are authorized to manufacture ID cards must be subject to “appropriate security clearance requirements.” It is not clear what standards states should set in disqualifying employees or hiring new employees. The fact that some states contract with private entities for ID production further complicates this issue. (<i>“Real Burdens”</i>) The regulations do set down clear standards for state employees who should be checked: those who “have the ability to affect the recording of any information required to be verified, or who are involved in the manufacture or production of REAL ID driver’s licenses and identification cards, or who have the ability to affect the identity information that appears on the driver’s license or identification card” (p. 10,856). They also make clear what the standards of those checks should be: those set forth in TSA’s Hazardous Materials Endorsement program (HAZMAT program) and Transportation Workers Identification Credential (TWIC) program (p. 10,840).</p>
PASS <input type="checkbox"/> FAIL <input type="checkbox"/> INC <input checked="" type="checkbox"/>	<p>Security clearance and labor contracts. Security clearance requirements may run afoul of contract stipulations and union rules. States may need to provide employees disqualified under new regulations with alternative employment or severance. (<i>NCSL et al, “Impact Analysis”</i>) The regulations are incomplete because they do not address how workers’ collective bargaining agreements will affect whether they can be asked to undergo background checks.</p>
PASS <input type="checkbox"/> FAIL <input type="checkbox"/> INC <input checked="" type="checkbox"/>	<p>New training requirements. Under Real ID state employees must undergo “fraudulent document recognition training programs.” It is not clear what these programs entail or the impact on the cost of issuing licenses. (<i>“Real Burdens”</i>) The regulations do saddle DMVs with the increased cost and burden of training employees in fraudulent document recognition without providing any funding. They do not elaborate on this training requirement except to affirm that it must be part of every DMV security program (p. 10,855). It is expected to take approximately 2 hours and cost \$44 per person in lost man hours (p. 10,846).</p>
Constitutional Impact	
A. Burdens on constitutional rights of the states.	

PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Federalism and the Tenth Amendment. States have always been the exclusive regulator of driver licensing. Each state has developed an extensive statutory and regulatory framework in this area, and each state employs workers to carry out that statutory and regulatory scheme. The Tenth Amendment provides that “[t]he powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively” The REAL ID Act seizes the power reserved for the states by federalizing drivers licensing. Real ID was vigorously opposed by the organizations representing the states and seems to violate the Tenth Amendment. (<i>See ACLU analysis, “Constitutional Problems with the REAL ID Act of 2005”</i>) The regulations violate the Tenth Amendment by seizing state authority over licensing and by forcing states to engaged in regulation on behalf of the federal government. The regulations argue that Real ID does not violate the Tenth Amendment because the burden will fall on citizens rather than on “the State as a sovereign.” This is an incorrect reading of the law. The test under existing law is whether a state (as sovereign) has been compelled to adopt a federal program, not whether the program acts directly on the state. The regulations do not address the states’ traditional authority in the field of drivers licensing.</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>The Anti-Commandeering Doctrine and the Tenth Amendment. The REAL ID Act requires states driver’s licensing officials to perform two exclusively Federal functions: enforcing immigration laws and creating a federal ID card. Constitutional and statutory schemes governing immigration law make clear that immigration enforcement is entirely a Federal function. Additionally the Real ID Act turns state drivers’ licenses into Federal identity documents, necessary for official purposes like entering a Federal facility. According to the Supreme Court’s anti-commandeering doctrine, if the Federal government wants to conduct interior immigration enforcement or create Federal identity cards it must hire and pay Federal government employees to do so, rather than forcing states’ licensing employees to carry out this activity. (<i>“Constitutional Problems with the REAL ID Act”</i>) The regulations do not address the main constitutional issue: whether imposing penalties on citizens when states don’t act amounts to a violation of the Anti-Commandeering doctrine. The regulations claim that “the proposed rule would not formally compel any State to issue driver’s licenses or identification cards that will be acceptable for federal purposes” and instead that it is pressure on individual citizens that will force compliance with Real ID (p. 10,849). But this doesn’t answer the main question: if a state can only reject federal law at the expense of denying its citizens access to basic aspects of American life like entering a federal facility or traveling on a plane, does this rise to the level of coercion necessary to trigger constitutional scrutiny?</p>

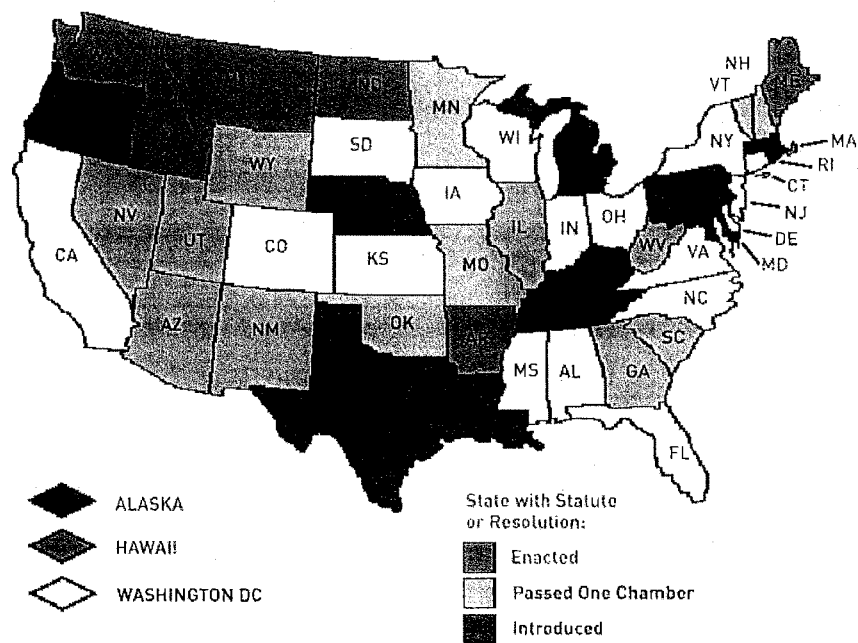
B. Burdens on constitutional rights of individuals.		
PASS	FAIL	INC
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Free exercise of religion and the photo requirement. Real ID requires, without exemption, that a digital photograph appear on each ID. This requirement violates the religious beliefs of Amish Christians, Muslim women and others and impacts the free exercise of their religion. (<i>"Constitutional Problems with the REAL ID Act"</i>) The regulations affirm that in order to receive a Real ID, every applicant must have a photo taken. It acknowledges individual religious objections but states that security requirements override those objections (p. 10,835).</p>		
PASS	FAIL	INC
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Free exercise of religion and Social Security numbers. Some Christian sects believe that "the enumeration" of individuals is tantamount to stamping them with the Mark of the Beast referred to in the Biblical Book of Revelations. Therefore due to these religious beliefs, certain citizens may not have the Social Security Number or Social Security Card necessary to gain a Real ID. (<i>"Constitutional Problems with the REAL ID Act"</i>) The regulations do not provide for a religious exemption in this context. They require that every applicant for a license have a Social Security number. The only way under to establish ineligibility for an SSN is for an alien to "present evidence that he or she is currently in a non-work authorized nonimmigrant status" (p. 10,852).</p>		
PASS	FAIL	INC
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Gender designation requirement. Real ID requires inclusion of each person's gender on his or her license. Many states and municipalities recognize the unique difficulties faced by issuing identity licenses to transgender people, and, accordingly, provide for exceptions to gender-listing requirements. The act would preempt those exceptions and may violate of the Constitution's Equal Protection Clause for transgender individuals. The gender classification will also lead to data inconsistencies within the databases that will "red flag" transgender people when their licenses are scanned by government officials. (<i>"Constitutional Problems with the REAL ID Act"</i>) The regulations do not address this issue because they fail to ensure the security of personal data, which is of particular concern to transgender individuals given that the disclosure of such data may subject them to harassment and other forms of discrimination.</p>		

PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Burdens on right to travel. The U.S. Supreme Court has repeatedly recognized a constitutionally protected right to travel. By ruling a state out of compliance the federal government may keep a state's residents from boarding a plane and possibly other modes of transportation, which would likely burden their First Amendment-protected right to travel. The situation is particularly acute for residents of Hawaii or Alaska who often have no choice but to fly or travel via federally regulated modes of travel such as plane or ship. (<i>"Constitutional Problems with the REAL ID Act"</i>) The regulations affirm that after the effective date of the act, a Real ID will be required to board a plane (p. 10,851). They do not address the constitutional issue.</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Burdens on right of assembly. The First Amendment protects "the right of the people to peaceably assemble." Blocking individuals from non-compliant states from using their licenses to enter federal buildings seems to burden that right. (<i>"Constitutional Problems with the REAL ID Act"</i>) The regulations affirm that after the effective date of the act, a Real ID will be required to enter a federal facility (p. 10,851). They do not address the constitutional issue.</p>
PASS FAIL INC <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Burdens on right of petition. The First Amendment also guarantees the right to "petition the government for a redress of their grievances." Lack of a Real ID compliant license would bar a citizen from a face-to-face meeting with his or her elected or appointed government representatives. In fact, many statutory and regulatory schemes <i>require</i> individuals to at times present themselves before elected or appointed officials to raise their grievances. Blocking individuals from entering their representatives' offices, Federal agencies or courthouses would be burden on the right to petition the government for redress. (<i>"Constitutional Problems with the REAL ID Act"</i>) The regulations affirm that after the effective date of the act, a Real ID will be required to enter a federal facility (p. 10,851). They do not address this constitutional issue or the related question of whether barring access to a courthouse, the ability to bring or defend a lawsuit or witness a court proceeding would also be prohibited under the Constitution.</p>

<div>PASS FAIL INC</div> <div> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>Lack of procedural or substantive due process. The Real ID Act fails to provide for a system for individuals to access government records about them, challenge inconsistencies and correct data errors concerning their files. The Real ID Act's failure to include a procedure whereby individuals can quickly, efficiently and permanently reverse data errors is likely to impact a number of substantive rights – such as receiving government benefits or boarding a plane – and violates the Constitution's guarantees of both procedural and substantive Due Process found in the Fifth and Fourteenth Amendments. (<i>"Constitutional Problems with the REAL ID Act"</i>) The regulations contain no appeal process for individuals who are confronted with errors in the information used to verify their identity. Instead individuals will have to correct errors with the database owners (pp. 10,833 & 10,852). The regulations do not address the constitutional issue.</p>
---	---

Appendix B

Status of Anti-Real ID Legislation in the States



Appendix C

Vermont news articles about Real ID

Appendix C.1.

“National ID System Expensive, Complicated,” editorial from *Burlington (Vt.) Free Press*, Aug. 27, 2006

Burlington Free Press

burlingtonfreepress.com | A LOCAL CUSTOM

National ID system expensive, complicated

States including Vermont, saddled with a 2008 deadline to implement a national identification system known as Real ID, are sending a clear message to Washington: Real ID is not well designed, cannot be implemented by 2008, and carries a crippling price tag for taxpayers.

The Bush administration fought successfully for the program to create uniform driver's license standards to improve identification at the borders and make it harder for terrorists to travel freely.

Under Real ID, drivers would appear at their state motor vehicle offices and present specific documents, such as birth certificates, to prove identity. The states would authenticate those documents, which might require new technology and personnel.

The driver's license system needs improvements. Federal officials should work with states to ensure those changes make sense, can be done in a realistic time frame, truly improve national security, and come with appropriate funding.

States aren't taking this mandate sitting down.

The National Governors Association and other groups are seeking flexibility and federal funding. Members of the National Conference of State Legislatures meeting in Nashville passed a resolution insisting Congress either fund the changes or repeal the requirements.

Last week, about 600 people from across the United States, Canada, Mexico and the United Kingdom attended the American Association of Motor Vehicle Administrators conference in Vermont to discuss Real ID, among other topics.

Vermont Motor Vehicles Commissioner Bonnie Rutledge told the Free Press on Thursday that this state cannot possibly meet a 2008 deadline. The new system would cost Vermont taxpayers more than \$2 million to implement, at a time when the state's transportation budget is too strapped to adequately pave roads or fix crumbling bridges.

Motor vehicle officials have suggested reasonable changes to Real ID. Among those, that states should be allowed to choose the material used for their licenses; requiring all states to use the same material would be expensive and make forgery that much easier, Rutledge argued.

In addition, officials recommended that drivers who have had licenses for at least 10 years should not be required to jump through all the hoops for a renewal. There are other changes suggested, as well.

Rutledge does agree with Homeland Security that all states should require licenses to include a photo. Some Vermonters might resist that, but the commissioner is probably right.

Improvements to the driver's license system are needed if these cards are going to continue to serve as identification for traveling Americans. However, Homeland Security needs to give states the flexibility and funding to design a system that truly works.

Appendix C.2.

“Federal Legislation – Real ID Act of 2005,” from *Vermont Privacy News*, Summer 2005

Federal Legislation -- Real ID Act of 2005

A new federal law known as the REAL ID Act of 2005 contains several provisions potentially harmful to the privacy interests of individuals, especially victims of domestic violence, who are in hiding or fleeing from abuse. REAL ID requires states to include the applicant's home address on every motor vehicle driver's license or identification card in order for that card to be accepted as valid by any Federal agency. Pub. L. No. 109-13 (H.R. 1268 Sec. 201, et seq.) No exception is provided for individuals who would be in danger as a result.

If a domestic violence victim does not have a valid license or identification card, she may not be able to access services essential to her safety, for example, commercial airlines or AMTRAK trains she may need to use to flee. She also could not obtain a US passport, enter a federal courthouse, or rent a US post office box.

Additionally, the law requires states to maintain a motor vehicle database that contains all data field printed on the license (including the home address) and to provide electronic access to all other States to information contained in the motor vehicle database. This provision could allow abusers who hack into the system to locate a victim anywhere in the country.

Vermont is currently one of 20 states that either do not require an address on a license or permit the applicant to use a post office box number or an address designated by the State's Secretary of State. Domestic violence victims have found this practice to be helpful as part of their safety planning. In addition, the Vermont Secretary of State's Office administers the Safe at Home program in which domestic or sexual violence victims can apply to use a post office box administered by the Secretary of State's Office as their official address. Approximately 100 Vermonters have been enrolled in the program.

Deputy Secretary of State, William Dalton, has expressed his commitment to continue the Safe at Home program "in accordance with State law" and to work with the legislature, the Governor and the congressional delegation to do whatever is necessary to address any problem that arose for victims using the program as a result of passage of the REAL ID act.

Appendix C.3.

"National ID Law Could Mean Problems for State," from *Rutland (Vt.) Herald* and *Barre-Montpelier (Vt.) Times Argus*, Jan. 14, 2006

National ID law could mean problems for state

By Louis Porter

MONTPELIER — A Homeland Security law setting national standards for driver's licenses could cause serious problems for Vermont's Department of Motor Vehicles and Vermont drivers seeking licenses.

A survey of motor vehicle officials nationwide about the Real ID Act found that the law could cost millions and hamper states' licensing efforts.

The same could be true in Vermont, said Howard Deal, the state DMV's deputy commissioner.

"It's not unique to Vermont," he said. "It is a nationwide problem."

Privacy advocates have long objected to the law, which would establish a national database of drivers.

"Vermont officials are right to be concerned," said Allen Gilbert, executive director of the American Civil Liberties Union of Vermont.

"Real ID not only means a national ID, but will likely mean higher taxes and fees, longer lines, repeat visits to the Vermont DMV, bureaucratic snafus, and, for a lot of people, the inability to obtain a license," he said. "To top it off, it will do little if anything to prevent terrorism."

Proponents of the Real ID program have said it is essential to stop terrorist attacks and to ensure that people are who they claim to be — when they visit federal buildings, for example.

Rep. James Sensenbrenner, R-Wisconsin, chairman of the House Judiciary Committee, has been a lead proponent of the measure.

"This sensible legislation is aimed at preventing another 9/11-type attack by disrupting terrorist travel and bolstering our border security," he said in May when the measure was passed as an attachment to a bill funding the war in Iraq.

The responses by Vermont's DMV in the fall survey, conducted by the American Association of Motor Vehicles, show that the Green Mountain State could have many of the same problems anticipated by officials in states around the country.

For starters, the databases of documents required to implement the program's requirements do not in many cases exist yet, Deal said. And, although the law was passed last spring, the rules governing specifically how it will be implemented may not be completed for some time, he said.

"We are still waiting for the rules," Deal said.

Those rules, needed to craft the databases, procedures and communication links to enact the program, may not be completed until 2007, even though the program is supposed to go into effect in May 2008.

"There is just so much to this act and any one aspect of it could be a significant job for a state the size of Vermont," Deal said.

While Vermont has fewer drivers than larger states, he said, it also has fewer DMV employees to do the work of setting up the new systems to verify and corroborate identification of those seeking to obtain or renew licenses and identity cards.

Another concern is that although the act mentions federal funding for the program, no specific pot of money has yet been set aside to pay for it, Deal said.

So far, states' estimates have far surpassed the federal government's estimated \$100 million reimbursement to the states.

Pennsylvania, for example, estimates the cost of the program will be \$85 million in that state alone.

Although Vermont's cost will be far less — about \$3 million by rough estimates — it will still be significant, Deal said.

He said that in addition to privacy concerns and cost, the Real ID law could affect how long it takes to be approved for and receive a driver's license. Every document, such as a birth certificate, will have to be verified.

"It's not going to be instantaneous response," he said.

Those requirements may also undo DMV's efforts in recent years to shorten wait times and lines at service counters, Deal said.

"We have significantly cut down wait lines at counters," he said.

If the program goes into effect as it is now set up, he said, "when an individual comes into our office to get their license or ID card, they aren't going to leave with it the same day."

The Real ID program may also conflict with a provision passed a few years ago when Vermont began requiring a picture driver's license, according to Sen. Richard Sears, D-Bennington. At that time a clause allowed drivers who did not want such a license to be grandfathered in, a measure that will likely conflict with federal requirements, Sears said.

Still, the day of a national identity card is probably coming, Sears said, like it or not.

"The feds have some great ideas, but they don't want to pay for them," said the chairman of the state's Senate Judiciary Committee. "It is kind of frustrating."

Gilbert sees Departments of Motor Vehicles from around the country adding to a coalition of groups opposing the Real ID law.

"Civil liberties groups, conservative groups, immigration groups — we've all been saying that Real ID will be a real disaster and needs to be revisited by Congress," Gilbert said.

Appendix C.4.

“Identity Guidelines Could Cost State \$8 Million,” from *Rutland (Vt.) Herald* and *Barre-Montpelier (Vt.) Times Argus*, May 3, 2007

Identity guidelines could cost state \$8 million

By Louis Porter

MONTPELIER — Implementing new federal requirements concerning how driver's licenses and identity cards are issued could cost Vermont \$8.5 million, not the roughly \$2 million originally estimated, a state official said.

States are now commenting on the proposed federal rules based on the 2005 Real ID Act. The specifics in those rules make it clear the cost of compliance with the act will be significantly more than the state had expected, said Bonnie Rutledge, commissioner of the Vermont Department of Motor Vehicles. Although the program could cost as much as \$23 billion nationally, states will have to pick up virtually all of that cost since there is very little federal funding for the program, Rutledge said.

Rutledge, who has been a leader of the American Association of Motor Vehicle Administrators on the issue, met with Homeland Security officials recently to talk about Real ID.

"I did come away with a much better feeling about homeland security listening to the concerns of the states," she said.

There is also a possibility that Vermont could follow Washington state's lead and eventually offer "enhanced" driver's licenses with a chip in them that could make crossing the Canadian border easier, she said.

Meanwhile, U.S. Sen. Patrick Leahy, D-Vt, is a co-sponsor of a bill that would repeal the Real ID Act and replace it with a previous system under which federal and state officials would gather to devise improvements in how driver's licenses are issued.

"He is concerned about the process that is leading to a costly mandate on states with too little input from states about the real world factors they will have to cope with in devising this system," said David Carle, spokesman for Leahy.

On May 8, the same day the comment period on the proposed rules ends, Leahy will hold hearings on the Real ID program, Carle said.

"He wants the committee to look squarely at the privacy implications for what amounts to

a national ID database," Carle said.

One concern about the program is that since databases of driver's licenses in each state would likely be linked, the security of the information in those registries could be compromised.

"Real ID is a dream of identity thieves and a nightmare for Americans," said Allen Gilbert of the American Civil Liberties Union of Vermont. "Because these systems are connected they are at risk of being taken by burglars or rogue officials."

Secretary of Homeland Security Michael Chertoff said in early March that the Real ID program is an important part of national security efforts. For applicants for driver's licenses to bring in documents verifying their Social Security numbers, date of birth and legal status is simply a matter of "common sense," Chertoff said, according to a news release.

"None of this stuff is top-secret stuff," he said. "We can't have a truly secure identification system based on driver's licenses unless we make sure that the states are protecting the information they are collecting as well as the places where the licenses are being produced and issued."

As for the cost of the program, the federal government has appropriated \$30 million and may provide more.

"I can't predict future budgets, but obviously we're mindful of the expense," Chertoff said.

But there are other problems in the Real ID rules as proposed, which Rutledge hopes will be fixed before they become final, she said.

For one thing, they require re-licensing all drivers and those drivers must bring in documents like birth certificates before they can get new licenses.

That is just silly in some cases, Rutledge said. For example, there is no reason for her father, who is 82 years old and lives in Duxbury, to track down his birth certificate after having a Vermont driver's license for most of his life.

"He lives across the street from the house he was born in," she said. "It makes no sense to ask someone like that to bring in identity documents again."

Another problem is the deadline for states to implement the changes, Rutledge said.

Although the Department of Homeland Security has offered states a chance to extend the deadline for their programs to be up and running, it is probably not long enough, especially for states with larger populations, Rutledge said.

"Even though they are allowing states to request an extension ... the extension will probably not meet the needs of the states," she said.

Rutledge said a driver's license with a chip that could be read electronically at the border could help Vermonters whose residency and history has been vetted cross into Quebec. Washington state and British Columbia are considering such a system now.

"We are a border state and do a lot with Quebec," Rutledge said. "You could pass freely across the border without a passport."

Such a driver's license could not be used for identification when flying, which requires a passport, she said.

Vermont lawmakers had been working on a bill to prepare for the implementation of the Real ID program in the state. But given the changes proposed for the program in Congress and the additional cost of the program, that measure has been put on hold for this year at least.

"There were too many problems with Real ID," Sen. Richard Mazza, D-Grand Isle, chairman of the Senate Transportation Committee, said. "I would rather see what happens in Washington (D.C.) before we take any action."

Rep. Richard Westman, R-Cambridge, chairman of the House Transportation Committee, said a driver's license with a chip could be a good idea.

"It would make it a lot easier for Vermont citizens to get across the border," he said. It also could greatly benefit Vermont ski areas if residents of Quebec could continue to cross the border easily, Westman said.

**Testimony of Jim Harper, Director of Information Policy
Studies
The Cato Institute
to the Senate Committee on the Judiciary
Will REAL ID Actually Make Us Safer? An Examination of
Privacy and Civil Liberties Concerns
May 8, 2007**

Chairman Leahy, Ranking Member Specter, and Members of the Committee:

It is a pleasure to speak with you today. I am director of information policy studies at the Cato Institute, a non-profit research foundation dedicated to preserving the traditional American principles of limited government, individual liberty, free markets, and peace. In that role, I study the unique problems in adapting law and policy to the information age. I also serve as a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, which advises the DHS Privacy Office and the Secretary of Homeland Security on privacy issues.

My most recent book is entitled *Identity Crisis: How Identification Is Overused and Misunderstood*. I am also editor of Privacilla.org, a Web-based think tank devoted exclusively to privacy, and I maintain an online resource about federal legislation and spending called WashingtonWatch.com. I speak only for myself today and not for any of the organizations with which I am affiliated or for any colleague.

* * * *

Mr. Chairman, the REAL ID Act is a dead letter. All that remains is for Congress to declare it so.

The proposed regulations issued by the Department of Homeland Security on March 9th, on which comments close today, help reveal that REAL ID is a loser. It costs more to implement than it would add to our country's protections.

The regulations "punted" on REAL ID's most important technology, security, and privacy problems. Of utmost importance, the DHS proposal lays the groundwork for systematic tracking of Americans based on their race.

Though the Department of Homeland Security failed to "fix it in the regs," this is not the agency's fault. Regulations cannot make this law work, and neither can delay. The real problem is the REAL ID law itself.

There are highly meritorious bills pending in the Senate and House to repeal the REAL ID Act and restore the identification security provisions that were passed in the 9/11-Commission-inspired Intelligence Reform and Terrorism Prevention Act. Congratulations, Mr. Chairman for being an original cosponsor of this legislation in the Senate.

These bills would be improved if they were to chart a path to government use of emerging digital identity and credentialing systems that are diverse, competitive, and privacy protective. We can have identification and credentialing systems that maximize security and minimize surveillance. REAL ID is the ugly alternative to getting it right.

REAL ID Does Not Secure the Country

I will begin with security issues, which are the most important. Simply put, the proponents of REAL ID have not borne their burden of proof. They have not shown that REAL ID would add to our country's protections — because it doesn't.

The Department of Homeland Security has had two years to articulate how REAL ID would work. But the cost-benefit analysis provided in the proposed rules issued in March (the notice of proposed rulemaking or "NPRM") helps show that implementing REAL ID would impose more costs on our society than it would provide security or other benefits. REAL ID would do more harm than good.

Executive Order 12866¹ requires agencies to assess the costs and benefits of the requirements they propose. In its cost-benefit analysis, the Department found that implementing REAL ID would cost over \$17 billion.² This is 50% higher than the \$11 billion estimate put forward by the National Conference of State Legislators.³

The NPRM was the Department's opportunity to show how REAL ID might add to our country's protections. But on the question of benefits, the Department of Homeland Security essentially punted. It said:

It is impossible to quantify or monetize the benefits of REAL ID using standard economic accounting techniques. However, though difficult to quantify, everyone understands the benefits of secure and trusted identification. The proposed minimum standards seek to improve the security and trustworthiness of a key enabler of public and commercial life — state-used driver's licenses and identification cards. As detailed below, these standards will impose additional burdens on individuals, States, and even the Federal government. These costs, however, must be weighed against the intangible but no less real benefits to both public and commercial activities achieved by secure and trustworthy identification.⁴

This is not analysis, of course. It is surmise. A few paragraphs later, it continues:

The proposed REAL ID regulation would strengthen the security of personal

¹ Executive Order 12866, Regulatory Planning and Review (Sept. 30, 1993), requires "significant regulatory actions," such as those costing over \$100 million annually, to be assessed in terms of benefits, costs, and alternatives.

² Id. at 10,845 (2006 dollars discounted at 7%).

³ National Conference of State Legislators, *NCSL News: REAL ID Will Cost States More than \$11 Billion* (Sept. 21, 2006) <<http://www.ncsl.org/programs/press/2006/pr060921REALID.htm>>.

⁴ See 72 Fed. Reg. 10844-46 (Mar. 9, 2007).

identification. Though difficult to quantify, nearly all people understand the benefits of secure and trusted identification and the economic, social, and personal costs of stolen or fictitious identities. The proposed REAL ID NPRM seeks to improve the security and trustworthiness of a key enabler of public and commercial life — state-issued driver's licenses and identification cards.

The primary benefit of REAL ID is to improve the security and lessen the vulnerability of federal buildings, nuclear facilities, and aircraft to terrorist attack. The rule would give states, local governments, or private sector entities an option to choose to require the use of REAL IDs for activities beyond the official purposes defined in this regulation. To the extent that states, local governments, and private sector entities make this choice, the rule may facilitate processes which depend on licenses and cards for identification and may benefit from the enhanced security procedures and characteristics put in place as a result of this proposed rule.

The assessment goes on to imagine what protection-rates would cost-justify the REAL ID Act regulations.⁵ According to the assessment, if REAL ID lowers by 3.6% per year the annual probability of a terrorist attack causing immediate impacts of \$63.9 billion, the rules would have net benefits. If REAL ID lowers by 0.61% per year the annual probability of a terrorist attack causing both immediate and longer run impacts of \$374.7 billion, the rules would have net benefits.

This is an unsound way of judging the anti-terrorism benefits of REAL ID, and it reflects almost no thinking about how REAL ID might work as a security tool. I have attached as Appendix A a rudimentary analysis of the REAL ID Act in terms of risk management, using the framework put forward by the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.⁶

To summarize, creating a national identification scheme would not just attach a known, accurate identity to everyone. It would cause wrongdoers to change their behavior. Sometimes this would control risks, sometimes this would shift risks from one place to another, and sometimes this would create even greater risks.

Rather than being evaluated on its ability to prevent attacks outright, as the NPRM did, the REAL ID Act should be assessed in terms of its ability to delay attacks or change their character. Assuming, for example, that a future attack would be on the scale of a 9/11 — an exaggerated assumption unless all the rest of our security efforts have done nothing — REAL ID might be assumed (generously) to delay such an attack by six months. The value of delaying such an attack, and thus the security value of REAL ID, ranges from \$2.24 billion to \$13.1 billion.⁷ REAL ID offers less in benefits than it does

⁵ This is permitted by OMB Circular A-4 when it is difficult to quantify and monetize the benefits of a rulemaking.

⁶ Data Privacy and Integrity Advisory Committee, U.S. Department of Homeland Security, *Framework for Privacy Analysis of Programs, Technologies, and Applications*, Report No. 2006-01 (Mar. 1, 2006).

⁷ Assumed delay from today until 6 months into the future. (Net present value at 3.5%/6 months interest.)

costs — even using very generous assumptions.

The NPRM concludes with this:

The potential ancillary benefits of REAL ID are numerous, as it would be more difficult to fraudulently obtain a legitimate license and would be substantially more costly to create a false license. These other benefits include reducing identity theft, unqualified driving, and fraudulent activities facilitated by less secure driver's licenses such as fraudulent access to government subsidies and welfare programs, illegal immigration, unlawful employment, unlawful access to firearms, voter fraud, and possibly underage drinking and smoking. DHS assumes that REAL ID would bring about changes on the margin that would potentially increase security and reduce illegal behavior. Because the size of the economic costs that REAL ID serves to reduce on the margin are so large, however, a relatively small impact of REAL ID may lead to significant benefits.

The actual economic analysis produced by DHS and placed in the rulemaking docket has some more specific information about "ancillary benefits." It estimates that REAL ID could reduce the costs of identity theft by merely \$1.6 billion during 2007-16.⁸ Relatively little identity fraud uses drivers' licenses. No other benefits are estimated.

In summary, implementation of REAL ID would cost over \$17 billion dollars. Its security benefits, under generous assumptions, might reach about \$15 billion. REAL ID promises 88 cents worth of security and "ancillary benefits" for every national security dollar we spend. These dollars would be taken from children's health care, from American families' food budgets, and from security programs that actually increase our protections. Implementing REAL ID would harm the country.

If REAL ID did add to our country's protections, it would not have been passed attached to a military spending bill two years ago. It would have had hearings, up-or-down votes in both houses, and fanfare at every step of the legislative process.

If REAL ID added to our country's protections, Americans would happily tolerate the expense, inconvenience, and intrusion created by the REAL ID system. They do not.

Securing the country is not controversial. REAL ID is controversial.

DHS Punted on the Hard Issues

The potential security benefit of having a national ID is the most important consideration. As we now see, REAL ID fails cost-benefit analysis. But there are additional costs of REAL ID that are not considered in the NPRM's cost-benefit analysis. These costs are denominated in the privacy and civil liberties of law abiding Americans.

⁸ Department of Homeland Security, *Regulatory Evaluation, Notice of Proposed Rulemaking, REAL ID* at 130 (Feb. 28, 2007)

Many states waited to see what they would find in the Department of Homeland Security's REAL ID regulations. Since DHS issued its regulations, many states have moved forward with anti-REAL ID legislation. I have attached as Appendix B a list of anti-REAL ID activity in the states since the regulations came out. On the toughest technology, security, and privacy issues, states have been left holding the bag. They do not want REAL ID, and for good reason.

Were they to comply with the REAL ID Act, states would have to cross a mine-field of complicated and expensive technology decisions. They would face enormous, possibly insurmountable, privacy and data security challenges. But the Department of Homeland Security avoided these issues by carefully observing the constraints of federalism even though the REAL ID law was crafted specifically to destroy the distinctions between state and federal responsibilities.

The Federalism Issue

The Constitution established a federal government with limited, enumerated powers, leaving the powers not delegated to the federal government to the states and people.⁹ Because direct regulation of the states would be unconstitutional,¹⁰ the REAL ID Act conditions federal acceptance of state-issued identification cards and drivers' licenses on their meeting certain federal standards.

This statutory structure — using state machinery to implement a federal program — is unfortunate. It blurs the lines of authority and obscures the workings of government from citizens and taxpayers. But it does draw federalism into play as a potential limit on the Department's ability to regulate.

As the Notice of Proposed Rulemaking notes,¹¹ Executive Order 13132 says that “issues that are not national in scope or significance are most appropriately addressed by the level of government closest to the people.”¹² Laying out the criteria for policymaking when federalism is implicated, the Executive Order says, “National action limiting the policymaking discretion of the States shall be taken only where there is constitutional and statutory authority for the action and the national activity is appropriate in light of the presence of a problem of national significance.”¹³

In support of a federal function — national security — the REAL ID Act conditions federal acceptance of state identification cards and drivers' licenses on their meeting federal standards for documentation, issuance, evidence of lawful status, verification of documents, security practices, and maintenance of driver databases. The federal government has equal power — and the Department of Homeland Security had discretion in this rule — to condition acceptance of identification cards and drivers' licenses on

⁹ U.S. Const. amend. X.

¹⁰ *New York v. United States*, 505 U.S. 144 (1992).

¹¹ 72 Fed. Reg. 10,820 (Mar. 9, 2007).

¹² E.O. 13132, Federalism (Aug. 4, 1999).

¹³ *Id.*

closely related priorities, including meeting standards for privacy and data security.

The decision not to do this is a policy question that, according to the federalism Executive Order, turns on whether there is constitutional and statutory authority and whether national action is appropriate. The Department's decision to abandon these issues to the states is an implicit finding that privacy and data security are not problems of national significance. That finding is wrong. Privacy is a problem of national significance.

Many different federal laws and policies seek to foster privacy and data security, even in the context of national security programs. The Executive Order establishing the President's board on safeguarding Americans' civil liberties, for example, states in its very first section:

The United States Government has a solemn obligation, and shall continue fully, to protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, in the effective performance of national security and homeland security functions.¹⁴

Among the many federal laws that are relevant is the Privacy Act of 1974.¹⁵ The Privacy Act requires federal agencies to undertake a variety of information practices, and it accords individuals a number of rights intended to protect privacy and similar interests. The law requires agencies to extend these protections to systems of records operated "by or on behalf of the agency . . . to accomplish an agency function" when that is done by contract.¹⁶

The Privacy Act did not contemplate that states would maintain systems of records in furtherance of federal functions. However, Office of Management and Budget guidelines issued after the Privacy Act's passage say that the Act is intended to cover "de facto as well as de jure Federal agency systems."¹⁷

Another relevant law is FISMA, the Federal Information Security Management Act of 2002.¹⁸ FISMA seeks to bolster information security within the federal government and for federal government functions by mandating yearly security audits. FISMA makes the head of each agency responsible for information security protections with regard to information systems and "information collected or maintained by or on behalf of the agency."¹⁹

REAL ID's Legislative History

The legislative history of the REAL ID Act suggests Congress' intention that the

¹⁴ E.O. 13353, Establishing the President's Board on Safeguarding Americans' Civil Liberties (Aug 27, 2004).

¹⁵ 5 U.S.C. §552a.

¹⁶ *Id.* at §552a(m).

¹⁷ Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities.

¹⁸ 44 U.S.C. § 3541 et seq. (enacted as Title III of the E-Government Act of 2002, Pub.L. 107-347).

¹⁹ 44 U.S.C. § 3544(a)(1)(A).

Department should implement REAL ID consistent with federal government policies on privacy. The Department of Homeland Security's Privacy Impact Assessment reviews relevant portions of that history:

The House Conference Report for the REAL ID Act includes several key statements of Congressional intent regarding privacy. For example, in its discussion of section 202(d)(12) of the Act, which requires each state to provide electronic access to the information in its motor vehicle databases to all of the other states, the Conference Report makes clear that Congress recognized the need for the regulations to address privacy and security and that those protections should be at least the equivalent of existing federal protections. The Conference Report reads in relevant part:

DHS will be expected to establish regulations which adequately protect the privacy of the holders of licenses and ID cards which meet the standards for federal identification and federal purposes.

In addition, the Conference Report discussion of Section 202(b)(9) of the Act, which calls for using "a common machine-readable technology, with defined minimum data elements," clearly indicates that Congress wanted privacy to be a consideration in implementing the technology. The Conference Report states:

There has been little research on methods to secure the privacy of the data contained on the machine readable strip. Improvements in the machine readable technology would allow for less data being present on the face of the card in the future, with other data stored securely and only able to be read by law enforcement officials.²⁰

REAL ID has Formidable Privacy and Data Security Problems

The privacy and data security consequences arising from REAL ID are immense, increasingly well understood, and probably insurmountable.

The increased data collection and data retention required of states is concerning. Requiring states to maintain databases of foundational identity documents will create an incredibly attractive target to criminal organizations, hackers, and other wrongdoers. The breach of a state's entire database, containing copies of birth certificates and various other documents and information, could topple the identity system we use in the United States today. The best data security is avoiding the creation of large databases of sensitive and valuable information in the first place.

The requirement that states transfer information from their databases to each other is concerning. This exposes the security weaknesses of each state to the security weaknesses of all the others. There are ways to limit the consequences of having a logical

²⁰ U.S. Department of Homeland Security, Privacy Impact Assessment for the REAL ID Act (Mar. 1, 2007) (footnotes and italics omitted) <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf>.

national database of driver information, but there is no way to ameliorate all the consequences of the REAL ID Act requirement that information about every American driver be made available to every other state.

There are serious concerns with the creation of a nationally uniform identity system. Converting from a system of many similar cards to a system of uniform cards is a major change. It is not just another in a series of small steps.

Economists know well that standards create efficiencies and economies of scale. When all the railroad tracks in the United States were converted to the same gauge, for example rail became a more efficient method of transportation. Because the same train car could travel on tracks anywhere in the country, more goods and people traveled by rail. Uniform ID cards would have the same influence on the uses of ID cards.

There are machine-readable components like magnetic strips and bar codes on many licenses today. Their types, locations, designs, and the information they carry differ from state to state. For this reason, they are not used very often. If all identification cards and licenses were the same, there would be economies of scale in producing card readers, software, and databases to capture and use this information. Americans would inevitably be asked more and more often to produce a REAL ID card, and share the data from it, when they engaged in various governmental and commercial transactions.

In turn, others would capitalize on the information collected in state databases and harvested using REAL ID cards. Speaking to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee in March last week, Anne Collins, the Registrar of Motor Vehicles for the Commonwealth of Massachusetts said, "If you build it they will come." Massed personal information will be an irresistible attraction to the Department of Homeland Security and many other governmental entities, who will dip into data about us for an endless variety of purposes.

Sure enough, the NPRM cites some other uses that governments are likely to make of REAL ID, including controlling "unlawful employment," gun ownership, drinking, and smoking. Uniform ID systems are a powerful tool. If we build it, they will come. REAL ID will be used for many purposes beyond what are contemplated today.

But the NPRM "punts" on even small steps to control these privacy concerns. It says for example that it "does not create a national database, because it leaves the decision of how to conduct the exchanges in the hands of the States."²¹ My car didn't hit you — the bumper did!

As to security and privacy of the information in state databases, the NPRM proposes paperwork. Under the proposed rules, states must prepare a "comprehensive security plan" covering information collected, disseminated, or stored in connection with the issuance of REAL ID licenses from unauthorized access, misuse, fraud, and identity theft.

²¹ 72 Fed. Reg. 10,825 (Mar. 9, 2007).

Requiring production of a plan is not nothing, and the NPRM refers to various “fair information practices.” However, preparing a plan is not a standard. The NPRM does not even condition federal acceptance of state cards on meeting the low standards of the federal Privacy Act or FISMA.

The REAL ID Act provided the Department of Homeland Security with very little opportunity to “fix it in the regs.” And DHS did not fix it in the regs. In fact, DHS created new concerns, such as the possibility of tracking by race.

REAL ID: The Race Card

The “machine-readable technology” required for every REAL ID-compliant card has been a subject of much worry and speculation. This is not without reason. A nationally uniform ID card will make it very likely that cards will be requested, and the data on them collected and used, by governments and corporations alike. DHS was wise to resist the use of radio frequency identification tags in REAL ID.²²

But even more significant issues have been created by the DHS’s choice of technical standards. The standard for the 2D barcode selected by the Department includes the cardholder’s race as one of the data elements.

If the REAL ID card is implemented, Americans transacting business using the REAL ID card may well be filling government and corporate databases with information that ties their race to records of their transactions and movements.

For the machine readable portion of the card, the technology standard proposed by DHS in the NPRM is the PDF-417 two-dimensional bar code. According to DHS, the PDF-417 barcode can be read by a standard 2D barcode scanner.²³ This is a more highly developed version of the barcode scanning that is done in grocery stores across the country.

The version selected by DHS is the 2005 AAMVA Driver’s License/Identification Card Design Specifications, Annex D. This is a standardized format for putting information in the bar code.

A summary of the data elements from the standard is attached as Appendix C, but briefly, white people would carry the designation “W”; black people would carry the designation “BK”; people of Hispanic origin would be designated “H”; Asian or Pacific Islanders would be “AP”; and Alaskan or American Indians would be “AI.”

²² The NPRM left the door for putting RFID chips in our identification cards in the future. See 72 Fed. Reg. 10,841-2 (Mar. 9, 2007). The DHS Data Privacy and Integrity Advisory Committee concluded recently that RFID is not well suited to the task of identifying people, at least at this stage in the technology’s development. Department of Homeland Security, Data Privacy & Integrity Advisory Committee, *The Use of RFID for Human Identify Verification*, Report No. 2006-02 (Dec. 6, 2006). The Department has recently cancelled RFID-related projects. See Alice Lipowicz, *DHS Tunes Out RFID*, Washington Technology (Feb. 12, 2007).

²³ 72 Fed. Reg. 10,837-8 (Mar. 9, 2007).

DHS does not require all the data elements from the standard, and it does not require the “race/ethnicity” data element, but the standard it has chosen will likely be adopted in its entirety by many state driver licensing bureaus. The DHS has done nothing to prevent or even discourage the placement of race and ethnicity in the machine readable zones of this national ID card.

Avoiding race- and ethnicity-based identification systems is an essential bulwark of protection for civil liberties, given our always-uncertain future. In Nazi Germany, in apartheid South Africa, and in the recent genocide in Rwanda, horrible deeds were administered using identification cards that included information about religion, about tribe, and about race. It took 60 years for the originally benign inclusion of ethnicity in the Rwandan national ID card to become a tool of genocide, but it happened all the same. Implementation of the REAL ID Act, which would permit race to be a part of the national identification card scheme, would be a grave error.

Akaka-Sununu is Essential — and it Needs a Vision of the Future

Congratulations again, Mr. Chairman on your leadership in cosponsoring legislation to repeal REAL ID and restore the ID security provisions from the 9/11-Commission-inspired Intelligence Reform and Terrorism Prevention Act.

REAL ID is often touted as a direct response to a strong recommendation of the 9/11 Commission. This is untrue on a number of levels.

The recent push for national ID cards is in reaction to the terrorist attacks of September 11, 2001, of course. An appendix to a report by the Markle Foundation Task Force on National Security in the Information Age recommended various governmental measures to make identification “more reliable.”²⁴ This report was cited by the 9/11 Commission as it recommended “federal government . . . standards for the issuance of birth certificates and forms of identification, such as drivers licenses.”²⁵ But it is important to know that the 9/11 Commission devoted about ¼ of a page in its 400-page report to identification issues. Identification security was not a “key finding” of the Commission.

Nonetheless, a provision of the Intelligence Reform and Terrorism Prevention Act of 2004, passed in response to the 9/11 Commission Report, established a negotiated rulemaking process for determining minimum standards for federally acceptable driver’s licenses and identification cards.²⁶ This provision — the result of the 9/11 Commission report — was repealed and replaced by the REAL ID Act. Restoring the earlier, more

²⁴ Markle Foundation Task Force on National Security in the Information Age, *Creating a Trusted Network for Homeland Security* (Dec. 2, 2003) <<http://www.markletaskforce.org/>>. The main body of the report endorsed the finding of the Appendix unconditionally. *See id.* at 36.

²⁵ National Commission on Terrorist Attacks Upon the United States (9-11 Commission), *The 9/11 Commission Report* (2004) at 390.

²⁶ Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458, §7212.

careful provisions would be a step in the right direction.

But the Congress should examine our country's identification policies and practices even more carefully. Identification systems have many benefits but, as we know from REAL ID, they also carry many threats. We should have a much more careful national discussion about the design of the identity systems we will use in the future.

There are identification systems being devised today by the countries' brightest technologists that would provide all the security that identification can provide, but that would resist tracking and surveillance. Meanwhile, hundreds of millions — if not billions — of taxpayer dollars are already being spent on government ID systems with little regard for their interoperability with emerging open standards, to say nothing of privacy.

It would be unfortunate if the federal government spent so much time and money to build systems that lead in a few decades to a very costly dead end. Even worse would be for government systems to predominate, making it a practical requirement that Americans do have to carry a national ID card in order to function.

As it moves forward, I recommend that the Akaka-Sununu legislation include consideration of emerging open standards for government IDs and credentials. Rather than being locked into the unwieldy federal systems now being created, federal agencies should have the flexibility to accept any identification card or credential that meets or exceeds government standards for data accuracy, security, and verifiability.

In Akaka-Sununu, Congress should recognize the emergence of identity and credentialing systems that are diverse, competitive, and — most importantly — privacy protective. These systems can maximize security while minimizing surveillance. REAL ID is the ugly alternative to getting it right.

APPENDIX A

Rudimentary Analysis of REAL ID Act in Terms of Risk Management

Assessing how, and how well, the REAL ID Act regulations benefit the homeland security mission in terms of risk management requires answers to the following questions. Answers available in the NPRM are critiqued here, and sensible or assumed answers are supplied:

- *What are you trying to protect?* The NPRM identifies federal buildings, nuclear facilities, and aircraft as the primary beneficiaries of the REAL ID rules, as well as other infrastructure should access to it be conditioned on showing ID. “Ancillary” beneficiaries would be the many segments of the public who would benefit from various types of fraud reduction, public safety law enforcement, and various forms of personal regulation.
- *What are you trying to protect it from?* The primary threat articulated by the rule’s brief benefit statement is “terrorist attack,” which can take any number of forms. The assessment does not describe with particularity any vulnerability or the way any of these assets may be harmed, much less how REAL ID would prevent or diminish such harm. As to ancillary beneficiaries, it is well known that fraud, unsafe behavior, and unwise personal choices have a variety of costs. The assessment does not describe how the REAL ID regulations would prevent these ills, though as part of an expanded police and regulatory state, they undoubtedly would.
- *What is the likelihood of each threat occurring and the consequence if it does?* The rule’s benefit statement makes no attempt at terrorism risk assessment, positing instead two different “9/11” scenarios, the avoidance of which would cost-justify the rules. The ancillary harms the assessment claims to effect vary widely across the landscape of human action, and have a variety of likelihoods and consequences.
- *What kind of action does the program take in response to the threat -- acceptance, prevention, interdiction, or mitigation?* The NPRM does not go into this kind of detail, but the REAL ID rules are best characterized as interdiction: a form of confrontation with, or influence exerted on, an attacker to eliminate or limit its movement toward causing harm. A more accurate and secure identification system may interfere with terrorists in a variety of ways.

Requiring REAL ID-compliant identification cards for access to secured areas would limit the field of potential attackers on those areas to only those people that are able to prove their identity and lawful presence in the United States. This would inconvenience foreign terrorist organizations, likely changing their behavior in a number of ways. The REAL ID Act might cause foreign terrorist organizations to target infrastructure that is not secured by identification requirements. It might cause them to select individual attackers who can lawfully enter the U.S. and acquire identification.²⁷ It might cause

²⁷ In general, this was the modus operandi of al Qaeda in the 9/11 attack.

them to ally with domestic criminals or criminal organizations.

They may attack the REAL ID system in various ways. The REAL ID regulations might induce foreign terrorist organizations to procure REAL ID-compliant cards through corrupt Department of Motor Vehicles employees. It might cause them to seek counterfeit documents that can fool DMV employees into issuing REAL ID-compliant cards. It might cause them to seek counterfeit REAL ID-compliant cards good enough to fool verifiers at checkpoints. It might cause them to corrupt verifiers at checkpoints.

Whatever the case, the REAL ID regulations would cause some inconvenience to foreign terrorist organizations seeking to mount an attack on infrastructure secured behind checkpoints.

A second form of interdiction, also not discussed in the NPRM, is the use of REAL ID in conjunction with watch lists. Again putting aside attacks on the REAL ID system, requiring REAL ID-compliant identification cards for access to secured areas would limit the field of potential attackers on those areas to only those people that are not known to be terrorists by the authorities. Coupled with watch lists, the REAL ID regulations might cause terrorist organizations, foreign and domestic, to target infrastructure that is not secured by identification requirements. It might cause them to select attackers who are not known to have contacts with terrorists.²⁸ It also might cause them to attack the REAL ID system in the ways discussed above.

Similar to the joining of REAL ID to watch lists in terrorism interdiction, REAL ID may be joined to a variety of commercial, law enforcement, and regulatory programs aimed at reducing fraud, promoting public safety, law enforcement, and various forms of personal regulation. Each of these multitudinous potential uses of REAL ID would alter the behavior of “attackers” in various ways. It would improve their behavior in some cases, inspire avoidance in others, and also in some cases prompt attacks on the REAL ID system like those discussed above, such as by college students seeking a good fake ID.

- *Does the response create new risks to the asset or others?* Some of the avoidance behaviors listed above would transfer risks or create new risks. Terrorists may shift from REAL-ID-secured targets to non-REAL-ID-secured targets.²⁹ Foreign terrorist

²⁸ As demonstrated by the “Carnival Booth” study, relevant information from watch lists is relatively easy to reverse-engineer. One must simply send an attacker through a checkpoint on a few “dry runs” to determine whether he or she is subject to different treatment. See Samidh Chakrabarti and Aaron Strauss, *Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System*, 6.806: Law and Ethics on the Electronic Frontier (May 16, 2002) <<http://www-swiss.ai.mit.edu/6095/student-papers/spring02-papers/caps.htm>>.

²⁹ Assuming terrorists aim to sap the economy and vitality of the United States, they could do very well by serially attacking non-ID-controlled targets if that would induce the U.S. to secure them through ID checks. If each of the 240 million licensed drivers in the U.S. were inconvenienced by just one minute per week to show ID at malls, subway stations, bus depots, office buildings, and other public infrastructure, the cost to society in lost time alone (assumed value: \$20/hr.) would be over \$4 billion per year – a net present cost of \$57 billion (assumed 7% interest).

organizations allying themselves with domestic criminal organizations to avoid REAL ID-based security might form more dangerous hybrid organizations. As noted above, there would certainly be attacks on the REAL ID system, in terms of technical security, corruption, fraud, and so on. The techniques developed by “casual” attackers such as college students would accrue to the benefit of the serious threats such as criminal or terrorist organizations. These are just some of the risk transfers and new risks that would result from implementing the REAL ID regulations.

APPENDIX B

Real ID Activity in the States Since Release of DHS Regulations

- **March 1:** Department of Homeland Security issues regulations, announces intention to extend deadline and acknowledges that Real ID will cost \$23 billion.
- **March 5:** New anti-Real ID legislation introduced in Arkansas; Washington Senate approves anti-Real ID legislation.
- **March 6:** New anti-Real ID legislation introduced in Pennsylvania; following a unanimous vote by the House, Idaho passes anti-Real ID legislation out of Senate committee.
- **March 7:** Illinois, South Carolina, Missouri and Hawaii all pass anti-Real ID legislation out of committee; Arkansas Senate passes a resolution calling on Congress to repeal Real ID; Utah sends anti-Real ID legislation passed in the Senate to the Governor's desk; Nevada introduces anti-Real ID legislation.
- **March 8:** Idaho Senate completes legislature's approval of resolution opting out of Real ID; Arizona Senate votes to opt out of Real ID.
- **March 9:** Texas introduces anti-Real ID legislation.
- **March 13:** Oklahoma House passes anti-Real ID resolution; Hawaii Senate passes anti-Real ID legislation.
- **March 14:** Oklahoma Senate passes anti-Real ID statute unanimously.
- **March 15:** Missouri House passes anti-Real ID legislation.
- **March 19:** Arkansas Senate passes additional anti-Real ID legislation.
- **March 20:** New Hampshire passes anti-Real ID legislation out of committee; Rhode Island introduces anti-Real ID legislation.
- **March 26:** Arizona House passes anti-Real ID legislation out of committee.
- **March 28:** Arkansas adopts two resolutions calling on Congress to repeal Real ID; Nevada Assembly passes anti-Real ID legislation.
- **April 3:** South Carolina Senate passes anti-Real ID statute.

- **April 4:** Tennessee introduces anti-Real ID legislation.
- **April 5:** New Hampshire House votes to opt out of Real ID.
- **April 13:** Alaska introduces anti-Real ID legislation.
- **April 17:** Montana enacts first statutory rejection of Real ID, formally opting out of the program.
- **April 18:** Washington enacts law to opt out of Real ID; Minnesota Senate passes anti-Real ID legislation.
- **April 19:** Illinois House passes anti-Real ID legislation unanimously; Georgia House passes anti-Real ID statute and sends it to the Governor's desk.
- **April 20:** North Dakota adopts a resolution calling on Congress to repeal Real ID; Colorado introduces anti-Real ID legislation.
- **April 21:** Oklahoma House unanimously approves Senate statute to opt out of Real ID.
- **April 25:** Hawaii adopts a resolution calling on Congress to repeal Real ID.
- **April 26:** Oregon House passes anti-Real ID legislation out of committee.
- **April 27:** Colorado passes anti-REAL ID legislation out of committee.
- **April 30:** Louisiana introduces anti-Real ID legislation.

APPENDIX C

From: Personal Identification — AAMVA International Specification — DL/ID Card Design, Annex D: “Mandatory PDF417 Bar Code”

MINIMUM MANDATORY DATA ELEMENTS

Jurisdiction-Specific Vehicle Class	Jurisdiction-specific vehicle class / group code, designating the type of vehicle the cardholder has privilege to drive.
Jurisdiction-Specific Restriction Codes	Jurisdiction-specific codes that represent restrictions to driving privileges (such as airbrakes, automatic transmission, daylight only, etc.).
Jurisdiction-Specific Endorsement Codes	Jurisdiction-specific codes that represent additional privileges granted to the cardholder beyond the vehicle class (such as transportation of passengers, hazardous materials, operation of motorcycles, etc.).
Document Expiration Date	Date on which the driving and identification privileges granted by the document are no longer valid. (MMDDCCYY for U.S., CCYYMMDD for Canada)
Customer Family Name	Family name of the cardholder. (Family name is sometimes also called “last name” or “surname.”) Collect full name for record, print as many characters as possible on front of DL/ID.
Customer Given Names	Given names of the cardholder. (Given names include all names other than the Family Name. This includes all those names sometimes also called “first” and “middle” names.) Collect full name for record, print as many characters as possible on front of DL/ID.
Document Issue Date	Date on which the document was first issued. (MMDDCCYY for U.S., CCYYMMDD for Canada)
Date of Birth	Date on which the cardholder was born. (MMDDCCYY for U.S., CCYYMMDD for Canada)
Physical Description — Sex	Gender of the cardholder. 1 = male, 2 =female.
Physical Description — Eye Color	Color of cardholder’s eyes. (ANSI D-20 codes)
Physical Description — Height	Height of cardholder. Inches (in): number of inches followed by “in” ex. 6’1” = “73 in” Centimeters (cm): number of centimeters followed by “cm” ex. 181 centimeters=“181 cm”

Testimony of Jim Harper, Director of Information Policy Studies, The Cato Institute, to the Senate Committee on the Judiciary
Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns
May 8, 2007

Address — Street 1	Street portion of the cardholder address.
Address — City	City portion of the cardholder address.
Address — Jurisdiction Code	State portion of the cardholder address.
Address — Postal Code	Postal code portion of the cardholder address in the U.S. and Canada. If the trailing portion of the postal code in the U.S. is not known, zeros will be used to fill the trailing set of numbers.
Customer ID Number	The number assigned or calculated by the issuing authority.
Document Discriminator	Number must uniquely identify a particular document issued to that customer from others that may have been issued in the past. This number may serve multiple purposes of document discrimination, audit information number, and/or inventory control.
Country Identification	Country in which DL/ID is issued. U.S. = USA, Canada = CAN.
Federal Commercial Vehicle Codes	Federally established codes for vehicle categories, endorsements, and restrictions that are generally applicable to commercial motor vehicles. If the vehicle is not a commercial vehicle, "NONE" is to be entered.

OPTIONAL DATA ELEMENTS

Address — Street 2	Second line of street portion of the cardholder address.
Hair color	Brown, black, blonde, gray, red/auburn, sandy, white
Place of birth	Country and municipality and/or state/province
Audit information	A string of letters and/or numbers that identifies when, where, and by whom a driver license/ID card was made. If audit information is not used on the card or the MRT, it must be included in the driver record.
Inventory control number	A string of letters and/or numbers that is affixed to the raw materials (card stock, laminate, etc.) used in producing driver licenses and ID cards.
Alias / AKA Family Name	Other family name by which cardholder is known.
Alias / AKA Given Name	Other given name by which cardholder is known
Alias / AKA	Other suffix by which cardholder is known

Suffix Name	Name Suffix (If jurisdiction participates in systems requiring name suffix (PDPS, CDLIS, etc.), the suffix must be collected and displayed on the DL/ID and in the MRT). Collect full name for record, print as many characters as possible on front of DL/ID.
Name Suffix	Indicates the approximate weight range of the cardholder: 0 = up to 31 kg (up to 70 lbs) 1 = 32 – 45 kg (71 – 100 lbs) 2 = 46 – 59 kg (101 – 130 lbs) 3 = 60 – 70 kg (131 – 160 lbs) 4 = 71 – 86 kg (161 – 190 lbs) 5 = 87 – 100 kg (191 – 220 lbs) 6 = 101 – 113 kg (221 – 250 lbs) 7 = 114 – 127 kg (251 – 280 lbs) 8 = 128 – 145 kg (281 – 320 lbs) 9 = 146+ kg (321+ lbs)
Physical Description — Weight Range	
Race / ethnicity	Codes for race or ethnicity of the cardholder, as defined in ANSI D20.
Standard vehicle classification	Standard vehicle classification code(s) for cardholder. This data element is a placeholder for future efforts to standardize vehicle classifications.
Standard endorsement code	Standard endorsement code(s) for cardholder. This data element is a placeholder for future efforts to standardize endorsement codes.
Standard restriction code	Standard restriction code(s) for cardholder. This data element is a placeholder for future efforts to standardize restriction codes.
Jurisdiction specific vehicle classification description	Text that explains the jurisdiction-specific code(s) for types of vehicles cardholder is authorized to drive.
Jurisdiction specific endorsement code description	Text that explains the jurisdiction-specific code(s) that indicates additional driving privileges granted to the cardholder beyond the vehicle class.
Jurisdiction specific restriction code description	Text describing the jurisdiction-specific restriction code(s) that curtail driving privileges.



**Improving Security *and* Protecting Privacy
Through REAL ID**

May 8, 2007

Executive Summary

Originally intended to certify competency to operate a motor vehicle, the typical American's driver's license today is used in the course of everyday activity as the most convenient and reliable document to authenticate personal identification. A driver's license is used to open a bank or credit account, to pay a retailer by check, to enter a commercial or government building, and to pass through security at airports and train stations. More than 80 percent of use their driver's license for purposes beyond driving.

Unfortunately, the value of a driver's license as a means of identification – combined with new technologies that facilitate the copying, forgery, fabrication and exchange of fraudulent driver's licenses – have benefited underage drinkers and smokers, criminals, and terrorists. Recognizing this danger, many states took action to inhibit forgery and tighten procedures for issuing driver's licenses. Then the use of fraudulent driver's licenses by the terrorists responsible for the tragic consequence of 9-11 compelled the federal government to develop safeguards for driver's license, as enacted by Congress in the REAL ID Act on May 11, 2005.

Two years later – and more than five years after 9-11, the debate continues to smolder over imagined threats to personal privacy from REAL ID. This ITAA White Paper outlines the background of the issue, explains how proven information technologies will improve security and integrity of American driver's licenses while also enhancing privacy protections for driver's data at every level.

ITAA strongly advocates federal and state government implementation of REAL ID without further delay. ITAA also offers other recommendations for the consideration of federal and state officials to ensure that security and privacy are maintained for future generations.

Evolution of the Driver's License

The earliest known driver's license in the United States was issued in 1903 in Massachusetts to help regulate the use and ensure the safety of the new technology of transportation by automobile.¹ By the 1930s, most state agencies had joined the Bay State in licensing their drivers. To qualify for a driver's license, applicants demonstrated the basic knowledge and skills required to safely operate a motor vehicle and were issued a "license" attesting to that fact. Early licenses were paper-based, with no photos or other security features. States began to add film-based photos in the late 1950s, and driver's licenses increasingly came to be used as a means of personal identification.

Today the state-issued driver's license is the most often used and most widely accepted identity document used to establish the holder's age and residence, make use of a check for payment, open a bank account, obtain credit, enter government and commercial buildings, board a plane, get a library card, and provide access to a wide array of other services and privileges – far beyond its intended purpose to certify an individual's qualifications to drive a motor vehicle. An April 2002 poll found that 83 percent of American citizens use their driver's license for purposes beyond driving.² Hence the driver license has become the *de facto* identification of choice used daily by most Americans. This makes it an extremely valuable document whose security is essential – along with the abilities to authenticate it and to share its information between law enforcement across jurisdictions. These requirements reflect the mobility of Americans, the widespread use of driver's licenses for purposes other than driving, and the growing abuse and costs to the public of illegally obtained driver's licenses.

Technology as Friend or Foe

Technology has advanced by leaps and bounds since that first driver's license was issued more than 100 years ago. As an unfortunate consequence, today's driver's licenses and their rightful owners have fallen victim to theft, forgery, and counterfeiting precisely because the driver's license *has* become such a valuable document for identification. New technologies in digital imaging and printing have made false driver's licenses easier to fabricate, and the Internet provides ready access to hundreds of vendors who sell ready-made fakes online.

This rise in counterfeiting has contributed significantly to the troubling growth of one of the most common and egregious violations of personal privacy – identity theft. According to a 2006 Federal Trade Commission report, consumer complaints of identity fraud and theft increased 25% between 2003 and 2005,³ with total economic losses to consumers of approximately \$5 billion and a total cost to businesses of over \$48 billion. In addition to the financial loss, it is estimated that last year it took consumers approximately 297 million hours to resolve identity theft issues.⁴ Fraudulent driver's licenses also enable illegal driving and underage drinking and smoking, and as Americans have become sadly aware, terrorism and other criminal activities.

As the tragic events of Sept. 11, 2001, demonstrated, our enemies will take full advantage of any loopholes and lax security in the issuing and authentication of driver's licenses. By one report, the 9-11 hijackers had obtained a total of 17 driver's licenses.

Some had duplicate driver's licenses. Backed up with other fraudulently obtained identification, the driver's licenses enabled the terrorists to use bank accounts, take flying lessons, rent cars and pass through airport security freely. This evidence led the 9-11 Commission to state in its final report:

Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers' licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.

Real ID is a direct result of these recommendations.

Restoring Security to Driver's Licenses

Well *before* the tragic events of 9-11, many state motor vehicle agencies had begun implementing changes to make driver's licenses more secure against the threat of identity theft and fraud through the use of digital photographs, micro-printing, barcodes, banknote style printing and other overt and covert security features. In September 2000, state representatives to the American Association of Motor Vehicle Administrators (AAMVA) voted 49 to 2 to institute the Driver License Agreement (DLA) in an effort to establish standards that would ensure a "One Driver, One License, One Record" system. In August, 2002, state representatives voted 48 to 3 to enhance the DLA by adding more security requirements. In 2004, a revised DLA was issued to and accepted by the states.

In the wake of 9-11, the U.S. government sought to expedite the *pace* of this change through federal standards that will migrate to more secure driver's licenses that will protect citizens' privacy and enhance national security.

Authentication and processing

The REAL ID Act, if implemented along the lines of the current Notice of Proposed Rule Making (NPRM) from the Department of Homeland Security, will substantially tighten both the data security and physical security requirements of state motor vehicle and driver's licensing offices, thus enhancing personal privacy by battling identity theft and fraud. REAL ID requires states to take new steps to verify the identity of applicants before issuing drivers' licenses and other ID cards. By December 31, 2009, state agencies will have to verify and authenticate birth certificates, social security cards and other source documents that individuals use to obtain drivers' licenses.

Although some states already have rigorous identity authentication procedures for enrollment of driver's license and other identification card applicants, the lack of minimum standards currently means that a state with insufficient or inconsistent procedures to authenticate applicants sets a lower denominator compared to states with better procedures. This attracts criminals and other abusers who can learn very easily which states have more lax requirements. The REAL ID Act sets clear requirements for

all states to ensure that documents presented to prove applicants' identities are authenticated. The documents standards for issuing a REAL ID driver's license or identification card will require states to improve fraud detection and to expedite authentication through verification from source document issuers. Technology enabled document and knowledge-based frameworks will facilitate this process until federal databases are online and fully available for authentication checks.

REAL ID also will require state authorities to share information with each other and to verify applicant data against existing federal databases such as the Social Security Administration, a step already taken by many states today. The DHS NPRM emphasizes the commitment to a "federated querying service" through which the states can access the federal reference databases in a "timely, secure, and cost-effective manner." However, DHS itself will not operate this service, and states can decide to go directly to the federal databases or use the existing AAMVANET service – a secure network owned and operated on behalf of state motor agencies by their professional association, the American Association of Motor Vehicle Administrators (AAMVA).

In addressing data sharing, *REAL ID does not establish or constitute a central, national database*, as many critics assert. To the contrary, it states a preference for a "pointer system" and assigns to the states the requirement to determine how they can best establish and secure linkages between themselves. The law, along with Senate-drafted conference language, directs the states to link their data systems to allow automated communication so that information contained in one state's system can be confirmed quickly by another.

Data exchange between states

Today a state's motor vehicle agency's computer system communicates with national systems such as the National Driver Register Problem Driver Pointer System, Social Security Administration and Commercial Driver License Information System to verify certain data, enforce safety programs, and keep records up to date. State motor vehicle data bases are closed systems (in contrast to open information systems searchable on the Internet) and access is limited to authorized users. The systems often are built on custom-developed data models and architectures with layered security components including "firewalls" to prevent unauthorized access via data links to these systems. The security access controls and firewalls, together with system intrusion detection software and audit capabilities, assure the safety of driver record information. The record shows that the data systems and computer programs associated with driver's system records are safe and secure, with an exemplary record of data security. Through the use of audit trails, a state can monitor access to information and prevent unauthorized data exchanges.

Unfortunately, gaps and vulnerabilities exist when it comes to sharing information from state to state. Although states use the Commercial Driver License Information System (CDLIS), the National Driver Register (NDR) or other programs to prevent duplicate or fraudulent licenses these systems only cover certain types of licenses and people intent on committing fraud exploit loopholes and the differences in state practices to obtain a false driver's license.

REAL ID will increase the barriers to issuing multiple licenses with real or fictitious information to the same person. To accomplish this, REAL ID requires all states to exchange certain data with all other states. At the same time, in its NPRM, DHS defers to the states to determine the design of the system to facilitate coordination between jurisdictions while safeguarding personal information. As stated in the NPRM:

The proposed rule seeks to address many of these (privacy) issues by leaving the operation of this data query, including the development of the business rules, to the States. The rule proposes to require individual States to document their business rules for reconciling data quality and formatting issues and urges States to develop best practices and common business rules by means of a collective governance structure.⁵

REAL ID security requirements also will make these driver's licenses and other IDs tamper-resistant and harder to forge.

Further Improving Privacy Through REAL ID

In its Notice of Proposed Rule Making (NPRM) on the REAL ID Act, the Department of Homeland Security makes its commitment to privacy very clear:

DHS believes that protecting the privacy of the personal information associated with implementation of the REAL ID Act is critical to maintaining the public trust that Government can provide basic services to its citizens while preserving their privacy. DHS recognizes the significant privacy issues that are associated with the Act.⁶

Where state-level systems are working well, REAL ID does not interfere with existing systems and procedures to protect privacy and ensure security. For example, REAL ID encourages the continuing use of the Commercial Driver License Information System (CDLIS) and the National Driver Register (NDR), whose data security records are unblemished. None of the opponents of the REAL ID Act and implementing regulations have raised a question about the protection of driver's license privacy in these systems.

REAL ID does take other important steps to *improve* the privacy protections of state driver's license applicant records, all within the existing authority of the federal government. The NPRM requires the states to report how they will maintain both data security and the physical security of the facilities where data is stored:

“...as part of the State certification mandated by section 202(a)(2) of the Act, each State will be required to prepare a comprehensive security plan for its DMV offices and driver's license storage and production facilities, databases, and systems utilized for collecting, disseminating or storing information used in the issuance of REAL ID licenses. As part of this requirement, DHS will require that each State include in its annual certification information as to how the State will protect the privacy of the data collected, used, and maintained in connection with REAL ID, including all the source documents.”⁷

By requiring states to certify and validate this certification on an annual basis, DHS will hold states strictly accountable for adherence to the highest data security and privacy standards, without dictating specific data security procedures. The required comprehensive security plans and annual recertification updates will give DHS the opportunity to recommend and oversee steps to continuously enhance the security and privacy of state programs as enabling technology evolve and any new threats are identified. For example, best practices can be shared regarding the best means to encrypt customer data during verification checks and to prevent unauthorized access to stored information. This new oversight, guidance on national trends and threats, and sharing of best practices will safeguard the privacy of Americans while also improving security.

Closer collaboration between states and the federal government, together with innovators in the information technology industry, will facilitate the integration of established technology measures that can be applied in a multi-layered approach to further improve security and enhance privacy protection. Examples include:

- Role-based security level systems that limit access to systems and data based on defined roles that can be set at the individual level;
- Enhanced business rules to control what users can do and to prevent corrupt data or incorrect transactions from entering the system;
- Use of data warehouses and reporting tools to look for anomalies that point to fraudulent activity;
- Web-based training and knowledge management tools to give employees better decision information;
- And document scanning and authentication technologies with the ability to authenticate documents such as birth certificates.

Nothing in the REAL ID Act or the NPRM will result in the federal government obtaining more information from driver records than exists today, nor is there additional information about the holders of driver's licenses that the federal government will be able to access or store. This fact is explained in detail in the NPRM, though it is often misinterpreted and misrepresented by many opponents.

From a privacy perspective, the greatest cost to an identity theft victim can occur when a state motor vehicle office, through weak controls or incomplete adjudication, issues a driver's license or identification card to a fraudulent applicant using a stolen Social Security number. There are tens of thousands of instances where identity theft victims have been charged with driving violations, crimes, and tax avoidance because a state has issued a valid identity document on the basis of a stolen Social Security Number, sometimes accompanied by the stolen name of the rightful holder of the Social Security Number. REAL ID will reduce these very harmful invasions of privacy by strengthening the authentication and verification process for issuing driver's licenses. Every step taken to increase security also contributes to privacy protection.

Added Privacy and Data Security Protection

The privacy and security of citizens personal information is one of the most important components of creating a secure identity management system. At the federal level, the

1994 Driver's Privacy Protection Act (DPPA)⁸ is the primary law that restricts how driver's license data can be used by states, and that law will continue to apply as REAL ID is implemented. DPPA bars states and their employees from selling or releasing personal information such as Social Security numbers, photographs, addresses, telephone numbers and birthdays, except under limited and legally prescribed circumstances. Should additional privacy protection be needed, the states should work with the federal government to strengthen DPPA to add greater protection of driver's license and identification document data.

DHS' NPRM correctly identifies existing vulnerabilities of data contained on the face of driver's licenses. DHS does not have authority to override state laws which provide open records. Because of the reported data-skimming activities of taverns and other commercial businesses, it would be wise for states to shift toward closed records. Alternatively, states can enact laws to ban retail establishments from capturing data from the face of IDs or from the machine-readable zone on the back of the card. The American Association of Motor Vehicle Administrators (AAMVA) has developed model legislation to prevent the capture and storage of information obtained from a driver's license or identification document. Some states have already barred such activities and have enforced the ban by establishing substantial fines for offenders, and in some cases, removing their liquor or retail licenses.

Conclusion: Real Privacy through REAL ID

Though not originally intended for this purpose, the driver's license has become the most commonly accepted form of identification for many purposes beyond driving motor vehicles. Because of these multifold usages, the driver's license has become the target for theft, counterfeit and falsification by thousands of abusers ranging from terrorists to young teenagers. Given these costs, including the tragic attacks of 9/11, steps must be taken to improve the security and reliability of driver's licenses.

Though printing and communications technologies have aided the abusers of driver's licenses, other proven information technologies are available today to give driver's licenses a new, much-needed level of security and integrity while also safeguarding the privacy of the individuals who make use of them daily.

By creating a minimum level of identity authentication, verification, and card security, REAL ID will improve security and privacy. States will continue to operate and control the state-to-state data exchange process and to verify records with federal databases.

REAL ID introduces no new threat to the privacy of Americans. In fact, its provisions will enhance that privacy, both directly and indirectly, by deterring identity theft and introducing new oversight of systems and procedures to protect personal information collected and stored at the state level. Every step taken to increase security also contributes to privacy protection.

Recommendations of ITAA

1. Congress, the Administration, and the States should fund and implement the REAL ID Act without further delay.
2. Once REAL ID programs are established, the federal government should help states continue to improve security and privacy as part of the annual recertification process. The information technology industry and other representatives from the private sector can contribute much to this on-going effort.
3. To enhance security at the state level, states that have not already done so should pass legislation to prevent the capture and storage of information obtained from a driver's license or other identification document. Such bans should be enforced with substantial penalties.

About ITAA

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 325 corporate members throughout the U.S. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, digital content, systems integration, telecommunications, and enterprise solution fields.

ITAA has an active identity management group. Our members include companies producing driver's licenses and other identity cards; managing federal, state and local smart card and identity credentialing programs; providing biometric devices, radio frequency identification technologies and middleware solutions; as well as performing background checks and other identity proofing services.

For more information, visit www.ita.org. ITAA also serves as secretariat of the World Information Technology and Services Alliance, consisting of 70 IT trade associations around the world.

Footnotes

¹ "Year of First State Driver License Law and First Driver Examination," Table DL-230 (June 1977), U.S. Department of Transportation, Federal Highway Administration, Highway Statistics Summary to 1975, U. S. Government Printing Office, Report No. HWA-HS-S75, p.71

² Public Opinion Strategies

³ Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data, January – December 2005*, January 2006

⁴ Federal Trade Commission, Overview of the Identity Theft Program, Sept 7, 2003

⁵ Notice of Proposed Rule Making, 4410-10, Department of Homeland Security, Office of the Secretary, 6 CFR Part 37, Docket No. DHS-2006-0030, RIN 1601-AA37, Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes p. 26

⁶ *Ibid*, p.32

⁷ Notice of Proposed Rule Making, 4410-10, Department of Homeland Security, Office of the Secretary, 6 CFR Part 37, Docket No. DHS-2006-0030, RIN 1601-AA37, Minimum Standards for Driver's licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes p. 27

⁸ Drivers Privacy Protection Act 18 U.S.C. § 2721 et. seq. (Public Law 103-322)

U.S. SENATE JUDICIARY COMMITTEE

**“WILL REAL ID ACTUALLY MAKE US SAFER?
AN EXAMINATION OF PRIVACY AND CIVIL
LIBERTIES CONCERNS”**

MAY 8, 2007

TESTIMONY OF JANICE L. KEPHART

FORMER COUNSEL 9/11 COMMISSION

PRESIDENT, 9/11 SECURITY SOLUTIONS, LLC

911SECURITYSOLUTIONS.COM

I. TESTIMONY OF JANICE L. KEPHART**II. QUICK FACTS ON *REAL ID* BY JANICE KEPHART****III. IDENTITY AND SECURITY: *REAL ID* AND THE STATES BY
JANICE KEPHART****IV. FEB. 2007 LETTER FRATERNAL ORDER OF POLICE RE
*REAL ID***

Chairman Leahy, Ranking Member Specter. Thank you for having me here today. It is an honor to be before you as an alum of the committee that prepared me so well for my work as a counsel to the 9/11 Commission. I appreciate very much this committee's continued interest and effort in the 9/11 Commission recommendations, including the issue of identity document security that *REAL ID* addresses head-on.

I am here in my own capacity today, but you should know that when the 9/11 Commission issued its final report card in December 2005, one of the highest marks it gave was to Congress for passing *REAL ID* legislation. Today, 9/11 Commissioner John Lehman works alongside me in our effort to get *REAL ID* implemented. I am also

happy to be one who speaks with the 70 percent of Americans who, in a recent Zogby/UPI poll, are in favor of secure driver licenses.

Today, every state DMV has taken at least a couple of steps towards REAL ID implementation. All DMVs check for commercial/problem drivers via the state-owned American Association of Motor Vehicle Administrators (AAMVA) network, AAMVANet. 48 states and DC check SSNs. 20 states check legal status. 3 states are sharing vital events digitized records, and 4 more are about to come online. Digital image access is available in 19 states and underway in 7 others. Alabama, New York and Texas are considered innovators in REAL ID compliance. In addition, at least 23 state legislatures have one or more bills pending supporting REAL ID in some fashion. Those that have passed REAL ID implementation or funding legislation through either their House or Senate include Arkansas, Indiana, Kansas, and Michigan.

In addition, I have written two papers on the subject, the first I published in February 2007 and sets out the policy backdrop for the REAL ID Act, explains its content, and discusses what is at risk if it fails. *Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security* emphasizes the need for security at the base of the nation's identity document issuance processes. The second paper, *Identity and Security: REAL ID in the States*, answers policy concerns being echoed in some states regarding REAL ID implementation. Both papers are attached.

REAL ID was passed into law based on the states' own Secure Document Framework developed by AAMVA after the states acknowledged post 9/11 that the current state driver license issuance system is deeply flawed in its ability to generate IDs both secure in their content and production. Such deep weaknesses threaten national and economic security, public safety, and our privacy.

The critical question this hearing asks, *Will REAL ID Actually Make Us Safer?* is absolutely the correct question to ask. The answer: an unequivocal 'yes'. If REAL ID is implemented, it will help individual Americans to preserve their identities, their children's safety in underage drinking and driving, and the police officer's ability to know who it is they are encountering on a day to day basis. The Fraternal Order of Police believes REAL ID would protect officers and apprehend criminals so much so that they have stated that any attempts to repeal REAL ID would result in pulling their support from a 9/11 implementation bill in this Congress. Their February 2007 letter to Majority Leader Harry Reid is attached.

As was discussed in much depth during an excellent *Terrorist Travel* hearing Subcommittee Chairwoman Feinstein held last Wednesday (May 2, 2007), secure IDs are essential for assuring people are who they say they are. That goes not only for travel documents, but all forms of IDs. Remember that the 9/11 terrorists—and many

other terrorists before them—had a travel operation that included the acquisition of state-issued IDs. (Discussed in depth in my Feb. 2007 paper.)

The 9/11 Final Report recommendations on terrorist travel called for action to “set standards for the issuance”¹ of state-issued identifications, including driver licenses, and “design a comprehensive screening system addressing common problems and setting common standards with system-wide goals in mind.”²

The 9/11 hijackers assimilated into the United States by attaining 17 driver licenses from Arizona, California and Florida (four of which were duplicates) and 13 state-issued IDs from Florida, Maryland and Virginia. The hijackers then used those IDs for the purpose of renting cars, obtaining living quarters, opening bank accounts, and boarding aircraft on the morning of 9/11. We know that at least six hijackers total presented state-issued IDs on the morning of 9/11. The pilot who flew into the Pentagon, Hani Hanjour, had ID cards from 4 states: Florida, Maryland and Virginia, and an Arizona driver’s license. The Pennsylvania pilot, Ziad Jarrah, had three IDs and an unverifiable ID when stopped for speeding two days prior to 9/11. Both pilots had obtained a Virginia ID by fraud.

In December 2005, the 9/11 Commissioners’ final report card on its recommendations gave Congress a good mark for passing into law solid language

¹ 9/11 Final Report, p. 390.

² 9/11 Final Report, p. 387.

pertaining to its identity security recommendations in the 2004 Intelligence Reform Act and 2005 REAL ID Act. However, the Commissioners remained concerned at the states' ability to comply, stating: "The REAL ID Act has established by statute standards for state-issued IDs acceptable for federal purposes, though states' compliance needs to be closely monitored."³

What has become unfortunate about the REAL ID debate is that myths and misinformation continue to abound. Let me address the most critical ones.

First, REAL ID is not a mandate. REAL ID preserves state rights. The REAL ID Act stipulates that in order for a driver license or state-issued ID to serve as an identity document for entering a federal facility— including boarding a plane— the document must meet, at a minimum, the security standards spelled out in the Act. Thus states are not required to issue licenses and IDs in accordance with REAL ID. The rules provide minimums, not a mandate. States can choose whether to comply or choose to exceed the minimum standards the law sets out. States keep control of issuing licenses, applicant data, and adjudication of applications. States can choose whether they will inconvenience their legal residents when they board planes or enter federal facilities by not providing them with a REAL ID; it is the federal government that is bound to only accept REAL IDs by the compliance date. Those that

³ 9/11 Commissioners Final Report on Recommendations (Dec. 2005).

choose not to comply will likely require their citizens to carry passports for such federal activities as boarding domestic flights.

Second, REAL ID does not create a national database. REAL ID does just the opposite, keeping data flows narrowly confined with only the originator of the data capable of holding the data. REAL ID enables verification of identity information such as SSNs, birth records, driving records, and immigration status between states and the federal government. The data is limited to defined fields of information with limited personnel access over a network owned and operated by the states, almost wholly through AAMVA. State to state interchange of information will continue to be up to the states. The states hold their own data and it is not acquired by any other entity. The same goes with the federal government.

Third, REAL ID does not invade privacy. The current REAL ID Notice of Proposed Rulemaking makes recommendations for best practices state should employ to protect privacy through stronger identity authentication. These best practices are hefty and build on the Commercial Driver License Information System (CDLIS) and National Driver Register (NDR) database created in 1986. These databases together have been servicing 45 states for 20 years. There have been no complaints about intrusions on privacy or identity theft with either of these databases. One reason why is because federal law already protects the use of such data under the Driver's Privacy

Protection Act of 1994. This law restricts how driver license information can be used by states, barring states and their employees from selling or releasing personal information such as SSNs, images, addresses, phone numbers and birthdates. Until that law was passed, 35 states had such information public and many made money off the sale of such information to all varieties of private enterprise. Congress set a higher bar to protect privacy in the area of state-issued driver licenses then, and REAL ID 20 years later is a natural follow-up: not only securing data, but identities and the documents that support those identities as well.

In part due to the success of the CDLIS and NDR in providing solid data without privacy breaches, this CDLIS and NDR system today accessed via AAMVAnet is likely to be the foundation for other identity verification and document authentication requirements under REAL ID.

REAL ID also provides greater protection of privacy, requiring background checks of DMV employees, secure productions sites of cards, alongside due respect to civil liberties. Just to be clear, there are no plans for an embedded RFID chip in REAL ID driver licenses.

Also worthy of mention is that the Information Technology Association of America, who represents the largest producers of computer security systems—IBM, Microsoft, Hewlett Packard, Oracle and others—has concluded that REAL ID, if

implemented, will further protect privacy. In a May 7, 2007 report (yesterday), the ITAA stated that REAL ID will actually “raises the bar on privacy for driver licenses” because it sets higher benchmarks for data security; requires tougher identity adjudication; and builds on existing practice.

Fourth, REAL ID does not create a National ID Card. REAL ID, in fact, avoids a national ID card. States use and control their own issuance processes, including meeting or exceeding REAL ID minimum standards. Calls for pull back or repeal will only make the debate surge again for proponents of a national ID.

To make REAL ID a reality requires more than either the federal government or the states can do on their own. It requires partnership. It also requires an acknowledgement that securing our nation’s physical and economic integrity is not just a federal responsibility; it is everyone’s responsibility. No REAL ID simply keeps us right where we are—vulnerable. The Congressional lobby we need now is for more seed money to help states comply with REAL ID, including built-in incentives for states that do so. Resolution of *this* issue is what gets us closer to secure IDs sooner rather than never.

QUICK FACTS IDENTITY AND SECURITY: REAL ID (1 of 2)

Janice Kephart, former counsel 9/11 Commission and president, 9/11 Security Solutions LLC

Historical background for REAL ID stems from two main sources: the 9/11 Commission and AAMVA.

9/11 Commission recommendation stated *Secure identification should begin in the United States. The federal government should set standards for ... sources of identifications, such as driver licenses.* The Commission recognized this recommendation would require a partnership between the federal gov't and the states as state-issued DLs/IDs are now the IDs of choice by banks, credit card companies, entertainment industry, airlines, federal facility entry.

AAMVA and AAMVAnet provide the technical backbone to state DMV driver license (DL) and ID issuance. AAMVA's Security Document Framework was the base for the language of REAL ID in recognition of 9/11 Comm'n criticisms. Their AAMVAnet supports data exchange b/w the fed gov't and states to check commercial driver records, SSNs and--in some states-- vital events and digital image verifications.

Policy background

National security. The 9/11 hijackers had 30 state-issued IDs. Only one hijacker did not. Many had multiple DLs/IDs from various states including the Pentagon and PA pilots. Other terrorists have held multiple IDs as well, including Kansi (1993 CIA shootings) and al-Marabh (2000 Jordanian plot).

Economic security. In 2005, \$18.1 billion in id theft related to DLs. Alien smugglers take advantage of weak ID issuance systems. Counterfeiting rings steal millions a year.

Public safety. Deadbeat dads, underage drinkers and drivers, criminals, bad drivers all take advantage of multiple IDs to cover their identity and tracks.

REAL ID defined

Not a mandate, but an opt-in for states that choose to comply with minimum standards.

REAL ID DL/IDs must be presented to enter a **federal facility**, including a commercial aircraft.

Elements of compliance: applicant documentation to establish identity; verification requirements, including one driver/one license; info on DLs/IDs; security features on card; security of card production; employee background checks; state certification of REAL ID compliance by DHS; database connectivity.

Cost was estimated by the NGA/NCSL/AAMVA at \$1 billion start-up, \$11 billion full compliance. DHS estimate \$14.6 billion but think amount lower once regs finalized. \$34 million still unreleased. States are allowed to spend 20 percent of the federal homeland security grants. Asst Sec Barth: DHS will try to help states to cut costs, by doing procurements at "the lowest possible cost." House HSC has authorized \$300 million.

Deadlines include May 8, NPRM comments due. DHS looks to finalize rule by Aug/Sept 2007. State compliance by May 8, 2009. Extensions encouraged by DHS.

State activity

DMVs. All DMVs are making progress in securing their DL/ID issuance processes in one area, many in multiple areas. All check for commercial/problem drivers via AAMVAnet. 48 states and DC check SSNs. 20 states check legal status. 3 states are sharing vital events digitized records, and 4 more are about to come online. Digital image access available in 19 states, underway in 7 others.

State Legislatures. 23 have forward momentum. 3 states seek full REAL ID implementation. 4 have enacted memorials to repeal. At least 6 have multiple pending bills both for and against.

QUICK FACTS IDENTITY AND SECURITY: REAL ID (2 of 2)

Debunking Myths

National ID Card. Not a mandate and no requirement to comply; states use/control own issuance processes, including going beyond REAL ID minimum standards.

Privacy. States must submit privacy plans and under REAL ID there is no collection nor release of personal data. No complaints that current REAL ID-compliant verification violates privacy. No RFID planned in DLs.

National database. No federal database exists and AAMVA provides most networking b/w fed databases and states. States will continue to hold their own data, which is provided upon query only in defined fields.

States' rights. Only imposes requirements on the fed gov't, not the states, nor will fed gov't issue licenses. State-to-state information exchange is up to the states.

IDENTITY AND SECURITY: *REAL ID* IN THE STATES

By Janice L. Kephart

*Former Counsel to the 9/11 Commission
President, 9/11 Security Solutions, LLC
911securitysolutions.com*

April 2007

IDENTITY AND SECURITY:

REAL ID IN THE STATES

This joint memorial is for the purpose of sending a message to Congress and to our Congressional Delegation that the people of Idaho object to the mandates of the Real ID Act of 2005 passed by Congress. The Real ID Act of 2005 is an \$11 billion unfunded mandate on the states. The Real ID Act of 2005 is a backdoor attempt to institute a national ID card as more overt attempts to create a national ID card have always failed in the past.

The Real ID Act of 2005 has serious constitutional and privacy problems. By requiring all states to issue driver's licenses to this new standard, the Federal Government is attempting to force the states to become part of a national database with 50,000 access points to sensitive data on every American Citizen. The opportunities for identity theft will multiply exponentially. Rules for implementing the Real ID Act of 2005 have not yet been promulgated by the federal government and the states are unclear as to the actual expected cost of compliance.

Idaho Joint Memorial, March 12, 2007

Introduction

REAL ID is one of the only 9/11 Commission recommendations that relies heavily on the states for implementation. REAL ID might have curtailed 9/11. REAL ID can make a difference to our national security, our economic security and our public safety – but only if fully implemented and adequately funded. To make REAL ID a reality, however, requires more than either the federal government or the states can do on their own. It requires a partnership. It also requires an acknowledgement that securing our nation's physical and economic integrity is not just a federal responsibility; it is everyone's responsibility. It requires a further acknowledgement that the ability to verify an individual's true identity is one of the cornerstones of national and economic security.

The REAL ID Act stipulates that in order for a driver license or state-issued ID to serve as an identity document for entering a federal facility – including boarding

a plane – the document must meet, at a minimum, the security standards spelled out in the Act. Thus states are not required to issue licenses and IDs in accordance with REAL ID, but they could be subjecting their residents to considerable inconvenience if they do not. There is no intent whatsoever under REAL ID for the federal government to assume responsibility for issuing driver licenses. That process should and will remain with each state. REAL ID seeks only to ensure that every state's process for issuing driver licenses and IDs – including the documents themselves – meets specified minimum security standards. Determining precisely what REAL ID's minimum security standards will be is the purpose of the comment period now underway as part of the Notice of Proposed Rulemaking (NPRM) issued by the Department of Homeland Security (DHS) on March 1, 2007. That process concludes on May 8, 2007.

Today, 23 state legislatures have provided some forward momentum on REAL ID. Every state's Department of Motor Vehicles (DMV) is moving towards compliance with REAL ID in at least one area, and many are in multiple areas. The state of Washington has passed legislation not only to implement REAL ID but to go beyond it by instituting biometric checks on driver license applicants. Three states – Arkansas, Arizona and Colorado – have enacted or sent to their governor a request for Congress to fully fund REAL ID, although the first two express concerns about privacy. Nineteen states have pending legislation that seeks to implement REAL ID in some fashion. Oregon, for example, has five bills pending in support of REAL ID. Six states – Illinois, Maryland, Missouri, Nebraska, New Mexico and Vermont – have more than one piece of legislation pending that seeks either REAL ID implementation or repeal.

The mission of this paper is to give the 16 states like Idaho that seek the repeal or legislation akin to the repeal of REAL ID a reason to seek out federal partnership instead. It is essential that they do so; it takes all of us – the federal government, the states and individual Americans – to make this country the stronger, better America the 9/11 Commission envisioned when it issued its final report and recommendations and staff report *9/11 and Terrorist Travel*.

Why America needs secure driver licenses

At the foundation of the 9/11 Commission 'terrorist travel' recommendations on secure IDs was the basic understanding that terrorists will continue to easily assimilate within the United States as long as identity and identity document issuance processes are easily manipulated. The Commission stated:

All but one of the 9/11 hijackers acquired some form of U.S. identification document, some by fraud. Acquisition of these forms of identifications

would have assisted them in boarding commercial flights, renting cars, and other necessary activities.

Recommendation: Secure identification should begin in the United States. The federal government should set standards for ... sources of identifications, such as driver licenses.

Recommendation: The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with system wide goals in mind. (p. 390, 387)

As the 9/11 Commission noted, there was only one 9/11 hijacker who did not obtain some form of U.S. identification, whether a state-issued driver license,

THE CASE OF UNITED 93 PILOT ZIAD JARRAH

On September 9, 2001, two days before 9/11 pilot Ziad Jarrah crashed a plane nose-first into a field in Pennsylvania, Jarrah was stopped for speeding. This could have led to trouble for him, and trouble for the entire 9/11 operation, but it did not. Instead, Jarrah simply drove away with a \$270 speeding ticket. This would likely be the case today as well.

Why? Jarrah had obtained two driver licenses from the state of Florida – one on May 2 and the other on May 24, 2001. In addition, he fraudulently obtained a state-issued ID from Virginia on August 29. When he was stopped for speeding, we don't know which Florida license he presented to the officer.

Had REAL ID been in effect, Jarrah would have been limited to one active license and the officer could have checked for other violations. The officer could have checked an immigration database, which could have shown he had entered the U.S. illegally at least five times. Instead, the officer had none of this information. Jarrah got away with a

personal ID or both. Three of the five hijackers who crashed a plane into the Pentagon used fraudulently obtained licenses to board. The pilot of that plane had four IDs, all from different states, with at least one obtained by fraud. And if REAL ID had been in effect in 2001, the 9/11 operational ringleader and pilot that conducted the first World Trade Center suicide, Mohamed Atta, would only have been four days from having had an expired license when he was pulled over for speeding violation on July 5, 2001.

The 9/11 hijackers could have done the same today. It is still possible to obtain multiple licenses and IDs because identities are not verified. It's not only possible to game the system; it's likely, because states still don't exchange information with each other regarding those holding legitimate IDs. Police officers' hands are tied when they can't cross check the ID they've been handed against any other information.

The 9/11 hijackers are not the only terrorists we know of who have taken advantage of blind spots and weaknesses in ID issuance standards. One terrorist caught in 2001 on the northern border, Nabil al Marabh, had five driver licenses and a hazardous materials permit. Mir Aimal Kansi, who killed two people outside CIA headquarters in 1993, got a Virginia driver license despite being in the U.S. illegally. These same problems exist in many states today. As long as they do, terrorists will continue to take advantage of them.

In addition to terrorists, criminals of all ilk – identity thieves, counterfeiters, deadbeat dads and underage teens seeking IDs to drive and drive – also use multiple IDs to hide their true identity from the law. In 2005 identity theft costs were at a staggering \$64 billion, with \$18.1 billion of that cost involving theft of a Driver License (DL) or ID. Individual consumers spend an average of 330 hours trying to undo identity theft and suffer \$15,000 on average in losses. With REAL ID, identity theft will be much more difficult because of more secure IDs that will verify ID information before a DL/ID is issued and because the cards themselves will become more tamper-resistant and easier for law enforcement to determine fakes.

REAL ID Act Based on AAMVA's Security Document Framework

On October 24, 2001 the American Association of Motor Vehicles Administrators (AAMVA) – an organization promoting information exchange, uniform practices and reciprocity, with representatives from every US and Canadian jurisdiction – passed a resolution to form a special task force to enhance the security and integrity of the driver license and ID issuance processes.

Prior to 9/11, AAMVA had a significant leadership role that included petitioning Congress in 1996 to mandate minimum standards for driver licenses. From 1999 to 2001, AAMVA worked with the National Highway Transportation Administration (NHTSA) and Congress towards creation of the Driver Record Information Verification System (DRIVERs). So when AAMVA went to work on creating a special task force to deal with the panoply of issues involved in creating a more secure ID issuance framework, the organization had the ability and credibility to make a difference. And they did. Their work became the foundation for the technical requirements of the REAL ID Act.

The Driver License/ID Security Framework that emerged from the AAMVA Special Task Force was detailed and comprehensive; that Framework became the backbone for REAL ID. The outline of the task force responsibilities is worth

repeating as it shows how AAMVA – and thus the state DMVs – were well aware and desirous of fixing the multiple vulnerabilities in state ID issuances systems. In some ways, then, REAL ID was simply a federal bow to the states' own work in this area. AAMVA's 'Uniform Identification Subcommittee' divided the issues into sub-categories. What is interesting is that despite the permutation of the mission statements from these subcommittees to the AAMVA Security Document Framework, to REAL ID, to the proposed rules, much of the language and policy statements have remained relatively unchanged.

Another interesting aspect of AAMVA's tasking was a group established just to deal with enforcement issues, including those treating/ID fraud, and determine increased penalties for dealing with such fraud. A significant justification for REAL ID is that by setting minimum standards as a foundation in both the verification of identity and card production processes, security is built into all state systems. This will make law enforcement activity more effective while at the same time discouraging fraud. As Chuck Canterbury, National President of the Fraternal Order of Police stated in a Feb. 21, 2007 letter to Senate Majority Leader Harry Reid:

[REAL ID] is very much of an officer safety issue. Law enforcement officers need to have confidence that the documents presented to them to establish the identity of a given individual are accurate. Officers rely on these documents during traffic stops and other law enforcement actions to access information related to that individual's criminal history. No police officer wants to be in the dark about the fact that he may have detained a wanted or violent criminal who has simply obtained false identification. This places both the officer and the public he is sworn to protect in greater danger. For this reason, the FOP will strongly oppose any bill or amendment that would repeal the REAL ID Act.

Below is a chart that shows that the policies advocated by the states via AAMVA's 2001 working groups remains a strong influence on REAL ID policies advocated today by DHS and also influenced by the National Governors' Association and National Conference of State Legislators. This chart reflects where AAMVA started in 2001 as closely tied to March 26, 2007 testimony by DHS Assistant Secretary for Policy Development Richard Barth before the Senate Homeland Security and Governmental Affairs Committee.

Secure ID feature tasked	2001 AAMVA Secure ID Issuance Task Force assignments	2007 DHS REAL ID Proposed Rules for
-----------------------------	---	--

by AAMVA		Secure ID Issuance
<i>Model Legislation</i>	'develop model legislation to assist states in implementing the overall package of Uniform Identification Standards'	REAL ID is that legislation
<i>Process and Procedures</i>	'gather and incorporate all deliverables of the Uniform ID Subcommittee (Task Groups) into one Model Program. This model program will include minimum requirements, best practices and model legislation to support a uniform and secure driver license and identification card system for motor vehicle agencies in the U.S. and Canada.'	'At the end of the day, what does all this look like? While the rule is still pending, there is no definitive answer yet. However, the final answer is that the REAL ID standards will likely draw from all the best and most secure State practices already in place.' Richard Barth, testimony before the Senate HSGA, March 26, 2007.
<i>Driver License Agreement</i>	'The DLC/NRVC (Driver License Compact/Non-Resident Violator Compact) Joint Compact Executive Board has been asked to explore enhancing the newly created Driver License Agreement (DLA), a voluntary driver license compact between States, to include requirements established for a more secure DL/ID issuance system.'	
<i>DRIVERs Infrastructure</i>	'The Driver Record Information Verification System (DRIVERs) task group will be charged with creating an all driver pointer system, to keep bad drivers off the road. Simply put, DRIVERs will direct a state where to find and accurately verify someone's driving history in another state.'	
<i>Acceptable Documents</i>	'validate and update the existing acceptable ID document list for the proof/authentication of specific personal information, such as, name, date of birth (DOB), legal presence, etc. and evaluate the utilization of foreign	'states would require individuals obtaining driver's licenses or personal ID cards to present documentation to establish identity—U.S. nationality or lawful

<i>Residency</i>	documents for the same purpose. Phase two will result in a recommendation for document (DL/ID) validity periods in relation to legal status/validity' 'to develop a definition of residency/domicile with and without a legal presence requirement for the purpose of driver licensing (establishment of the driver control record) and identification. '	immigration status as defined by the Act, date of birth, SSN or ineligibility for SSN, and principal residence'
<i>Verification</i> <i>Fraudulent Document Recognition</i>	'identify and establish methods for verifying documents used to establish identity of an individual applying for a driver license or identification card. Verification of identity may include, but is not limited to, full legal name, date of birth, Social Security Number (when applicable), and residency and/or legal presence' 'to assist jurisdictions with the formal training of motor vehicle employees and law enforcement in the recognition/detection of fraudulent identification documents.'	'states would verify the issuance, validity, and completeness of a document presented. Electronic verification proposed depending on the category of documents' and include those to verify DOB, SSN, passport issuance and legal presence
<i>Card Design Specifications</i>	'deals with physical and encoded features of the driver license / ID document. Features include security elements, card layout, printed and encoded data, and machine-readable technologies. It is our hope that this effort produces a standard for the driver license document that specifies minimum data and minimum technologies to be used on the driver license / ID document'	'proposal contains standards for physical security features on the card designed to prevent tampering, counterfeiting or duplication for a fraudulent purpose, and a common MRT with defined data elements'
<i>Internal Controls</i>	'to identify best practices for internal fraud control and	<i>Physical Security/Security Plans:</i> 'each state must

	prevention measures	prepare a comprehensive security plan for all state DMV offices and DL/ID card storage and production facilities, databases and systems and submit these plans to DHS as part of its certification package. Congress has agreed since we have dealing with duplicate information or card production including full fingerprint and criminal data checks.
Oversight Compliance System	'to review current procedures for the oversight and compliance of Federal and State programs and to develop a process for compliance to AAMVA standards regarding DL/ID Processes/Procedures'	'similar to Dept Transportation regulations governing state administration of commercial driver licenses, states must submit a certification... to demonstrate compliance with.. [REAL ID] regulation"
Unique Identifier	<p>developing a way to uniquely identify an individual such that:</p> <ul style="list-style-type: none"> • A holder will have no more than one (1) DL/ID card and record • authorized users can verify that the holder of a DL/ID card is the individual to whom the card was issued, and • an individual's driver record contains only information that pertains to that individual. 	<p>state-to-state data exchange for those who possess REAL ID license, extending out the CDL's data exchange that has taken place since 1992, a program that eliminated multiple licenses in multiple states by 1992 (over 1,000) from 1992-1998.</p>

Debunking Myths

Idaho's joint memorial raises issues that are being replicated in jurisdictions across the nation. They deserve answers. This section attempts to do so with the caveat that the political, technological and security frameworks which exist today continue to mature as this paper is published.

The Real ID Act of 2005 is a backdoor attempt to institute a national ID card.

REAL ID was passed in part to do away with any notion of a National ID card. By seeking to set out minimum standards for the ID card already the ID of choice by financial, airline, entertainment and other sectors – the state-issued driver license or personal ID card – Congress made clear their intent to refrain from creating a national ID card. The only aspect of REAL ID that is national is the national interest that all states be set on a foundation of minimum standards; states can choose to meet none of them and not comply or they can choose to exceed those standards. Examples already exist on both sides of compliance, with states like Maine and Idaho currently opting out, and states like Washington already passing laws to exceed REAL ID minimum standards.

Far from calling for a national ID, fully implementing REAL ID is the best chance we have as a nation to prevent future calls for a national ID. However, implementing a national ID could become the default policy if REAL ID compliance does not occur in a comprehensive way. That makes the stakes a lot higher for all of us if states who say they will opt out actually do opt out.

The Real ID Act of 2005 has serious constitutional and privacy problems.

Constitutional issues

REAL ID does not usurp state power and does not violate the constitution. No state or other special interest has tried to file suit based on unconstitutionality because REAL ID requires nothing of the states. REAL ID instead imposes requirements on the federal government, requiring that only REAL ID compliant IDs be acceptable for official purposes. The NPRM limits the scope of "official purposes" of the credential to the uses specified in the REAL ID Act: (1) accessing federal facilities; (2) boarding federally-regulated aircraft; and (3) entering nuclear power plants. If states choose not to comply, DHS currently contemplates simply requiring that noncompliant state's residents carry other forms of identification for 'official purposes,' such as passports in combination with other documents.

In addition, the federal government will not issue the licenses or control the data provided by the applicants. The governance of state-to-state information exchange is completely up to the states, as well as how they decide to query any federal or private reference databases. States are already sharing best practices and moving toward standardization to enhance the security and

efficiency of their processes as well as the security and quality of state-issued credentials.

Privacy issues

REAL ID will not facilitate the collection or release of personal information to or by the DMV, the federal government, nor unauthorized persons within each state. Each state must submit a privacy policy to DHS as part of their Comprehensive Security Plan, including how data will be secured against unauthorized access and procedures for its maintenance.

There are legitimate concerns that states

DOCUMENT VERIFICATION is required under Section 202(c)(3)(A) of the REAL ID Act. All provide real time performance.

SSNs checked through SSOLV.

- Online since 1996
- Verifies name/DOB/SSN with the SSA
- Only provides match/no match information to requestor
- Averages 60,000 queries per day
- 47 jurisdictions participate
- 45 % queries processed in 1 second and 99.5% within 3 seconds
- While 87% match, the remainder do not, with 1.88% being clear fraud, or 1.128 per day on average

Vital events records checked through EVVER

- Pilot active since August 2004
- Verifies name/DOB/State of birth/record date with state Vital Records agencies via AAMVA net and EVVER network
- Over 76,000 records verified to date
- 3 states in pilot, 2 more to join in 2007, 2 others are digitized
- Match rate varies depending on state records, from 77% to 94%

Driver License/ID Card Document Verification System:

- Verifies name/DOB/DLN# /image request
- 8 states can conduct full verification, including images, and 41 others have begun the implementation process
- Relies on AAMVAnet

Immigration records checked through SAVE.

- Alien registration numbers or I-94 arrival/departure records used by states to query DHS
- States then rectify data provided by DHS with applicant records and make determination
- Currently a working group at AAMVA seeking to integrate SAVE into AAMVAnet
- Wisconsin added in April 1, 2007

employ best practices to protect personal data on applications, but DMVs have been dealing with that for years. In fact, under the 1994 Driver's Privacy Protection Act, states and their employees are barred from selling or releasing personal information such as Social Security numbers, photographs, addresses, telephone numbers and birthdays of applicants. The law was passed after a stalker murdered Rebecca Schaeffer, whose residential information was found through the California DMV. The statute was challenged by states who argued that Congress had overstepped its grounds by insisting upon privacy in public records and that the issue was within the states' purview. On appeal to the Supreme Court, the law was upheld under the commerce clause and the right of the federal government to regulate disclosures pertaining to privacy. This law still stands and must be incorporated into REAL ID implementation.

The dynamic for best practices of course changes and has new challenges when records go from paper to electronic. However, that is a challenge that continues to be faced – and continues to be aggressively addressed – in all electronic transactions.

On the federal level, these challenges are already being managed. When states today query both federal and private databases, authorized personnel receive responses only in defined fields of data absolutely necessary to verify essential information in regard to that particular query, whether the information sought is a SSN, a birth record, immigration or driving record. There have been no complaints that these queries and crosschecks have in any way compromised personal privacy. In fact, the checking of SSNs alone protects the privacy of legitimate applicants every day while bringing potentially illegitimate applications to attention.

The data called for on a REAL ID license is really no more than the best practices of most states. REAL ID requires that the DL or ID show the following information: full legal name, address of principal residence, digital photo, gender, date of birth; signature; issuance date; expiration date; unique document number (other than SSN); and machine-readable technology. Such information is essential for verifying identity when an ID card is presented.

Almost every state already requires this information, or nearly all of it, and US residents are accustomed to giving and holding such data on DL/ID cards. Individual state DMVs will continue to store driver license data, as will the cards, and the federal government will have no greater access to the information than it does currently.

It should also be noted that the common machine-readable technology required by the Act will not convert licenses into tracking devices. There is no requirement for a radio frequency (RF) ID chip or other such device that can scan data from a distance is contemplated in REAL ID. Instead, the NPRM proposes the use of 2-dimensional (2D) bar code technology already in use today by more than 40 DMVs. The information on this bar code is typically no different from what is readable manually on the face of the card.

The Federal Government is attempting to force the states to become part of a national database.

REAL ID does not propose a federal database holding masses of private data. The states will continue to hold their own data. What REAL ID does require is that a state verifies with the issuing agency that each document provided to prove identity is a valid document. Birth certificates, foreign passports and immigration documents are often difficult to authenticate. The REAL ID proposed rules contemplate fast, efficient and effective means to verify such data, mainly through electronic reference libraries. Four of these libraries already exist. One is in pilot. Another has yet to be developed. What is important to note is that none of these databases hold applicant data, and only one currently uses a government network to exchange information.

The network used today and considered for expansion is the privately owned and operated AAMVAnet, which will continue to be the network conduit for information flow between most federal government databases used to verify identity and determine eligibility for REAL ID applicants. AAMVAnet already acts as the network transferring data between federal and state authorities for commercial driver license and problem driver data (CDLIS and NDR); Social Security data (Social Security OnLine Verification (SSOLV)); vital events data pilot (Electronic Verification of Vital Event Records (EVVER)); and the Driver License/ID Card Document Verification System.

**VERIFYING IDENTITY
AND ADDRESSING
FRAUD**

In 2003, the New York DMV did a cross-check of SSNs provided by DL/ID applicants against the SSA database. At least 600,000 license or ID card-holders did not jive with the SSA's database.

A recent NC internal audit showed 27,000 DL/ID applicants used false SSNs, about half 'deceased' in SSA records.



A partly-burned copy of Ziad Jarrah's U.S. visa recovered from the Flight 93 crash site in Somerset County, Pennsylvania. Jarrah would have used this passport to obtain his two Florida DLs and his Virginia ID.

The only data exchanged directly between the federal government and the states right now are foreign resident legal presence checks under the US Citizenship and Immigration Service's data (SAVE), although an AAMVAnet solution is to be developed. There is current discussion that AAMVAnet would also be used for passport verification provided by the Department of State when that system is developed.

Importantly, states are already in significant compliance with many aspects of REAL ID's identity and eligibility verification requirements under REAL ID. All states are checking commercial driver and problem driver databases as required under prior federal law. All but two states are checking SSNs. Twenty states are checking for lawful presence. Vital effects (birth and death) records are in pilot within and between North Dakota, South Dakota and Iowa and five additional states have completed digitization of their vital effect records, including Hawaii, Iowa, Minnesota, Missouri and Montana. Colorado and Minnesota are scheduled to join the pilot in 2007.

What still needs to be developed are rules for data exchange between the federal and state entities, and state-to-state queries. Once again, however, this is doable, as such rules already exist for current data exchanges on driver applicants between federal and state partners. These rules can serve as the foundation for changes required under REAL ID as well, particularly those involving state-to-state exchanges. As long as the states implement this portion of the REAL ID Act, they – and not the federal government – will remain in control of the business processes. This is contemplated by DHS in their Privacy

Impact Assessment that was conducted pursuant to Congressional intent and published alongside the proposed rules for REAL ID.

The key will be to ensure that the states administer and manage the systems built to implement the Act. In addition, with appropriate and necessary participation from the affected federal agencies, including DHS, the Department of Transportation, and the Social Security Administration, the states must be empowered to develop the business rules surrounding the check of federal reference databases and the state-to-state data exchange processes. State, rather than federal, operation and control of the systems not only minimizes the appearance of a national database, but also fosters the system of federalism upon which our country is based. The language in the Preamble of the NPRM supports the important role of the states. (p.7-8)

Jurisdiction	CDLIS & NDR license checks	SSOLV (SSN)	SAVE (lawful presence)	EVVER (vital events)	Digital Image Access & Exchange
Alabama	✓	✓	✓		✓
Alaska	✓	✓			
Arizona	✓	✓			✓
Arkansas	✓	✓	✓		
Jurisdiction	CDLIS & NDR license checks	SSOLV (SSN)	SAVE (lawful presence)	EVVER (vital events)	Digital Image Access & Exchange
Colorado	✓	✓	✓		✓
Connecticut	✓	✓			
Delaware	✓	✓			
District of Columbia	✓	✓			✓
Florida	✓	✓	✓		
Georgia	✓	✓	✓		
Hawaii	✓	✓		✓	
Idaho	✓	✓	✓		✓
Illinois	✓	✓	✓		✓
Indiana	✓	✓	✓		
Iowa	✓	✓		✓	
Kansas	✓	✓			✓
Kentucky	✓	✓			✓
Louisiana	✓	✓			
Maine	✓	✓			
Maryland	✓	✓	✓		
Massachusetts	✓	✓			
Michigan	✓	✓			
Minnesota	✓			✓	

Mississippi	✓	✓			✓
Missouri	✓		✓	✓	
Montana	✓	✓		✓	
Nebraska	✓	✓			✓
Nevada	✓	✓	✓		✓
New Hampshire	✓	✓			
New Jersey	✓	✓	✓		
New Mexico	✓	✓			
New York	✓	✓	✓		
North Carolina	✓	✓			✓
North Dakota	✓	✓	✓	✓	✓
Ohio	✓	✓			
Oklahoma	✓				✓
Oregon	✓	✓			
Pennsylvania	✓	✓	✓		✓
Rhode Island	✓	✓			✓
South Carolina	✓	✓			
South Dakota	✓	✓	✓	✓	
Tennessee	✓	✓			
Texas	✓	✓			
Utah	✓	✓			
Vermont	✓	✓	✓		
Virginia	✓	✓	✓		
West Virginia	✓	✓			✓
Wisconsin	✓	✓	✓		✓
Wyoming	✓	✓	✓		✓

But for the last column, the chart above was part of March 26, 2007 DHS testimony before the Senate Homeland Security Committee detailing identity and document verification databases currently in use or implemented in states. The 'Digital Image Access' information was provided by AAMVA in a power point presentation during a Feb. 26-27, 2007 *Paving the Way for REAL ID* conference. Note that implementation for Digital Image Access is complete in 19 states, underway in seven states and feasibility start dates are under consideration in 16 states. Only eight states have no current activity in the area of digital image access verification.

While rules for data exchange need to be developed, what is clear is that many states are well on their way towards compliance with the identity verification portion of REAL ID in a manner that does not and will not create a national database.

The opportunities for identify theft will multiply exponentially.

A collateral positive side effect of REAL ID is that it will help curtail identity theft, not enable it. For legal residents, REAL ID requires stronger security features – the details of which are available for comment in the NPRM – with the intention of driving up the cost of creating counterfeit ID documents and enabling law enforcement both working with DMVs and in the field to make a quicker, more reliable determination of whether an ID is legitimate or not.

For criminals, terrorists and others who want to live in the U.S. for nefarious purposes or under false guise, obtaining a license or ID has been their ticket to acquiring legitimate cover for their illegitimate activities. Once our identity issuance systems and the IDs themselves are tightly secured, it will be much more difficult to obtain these "tickets" fraudulently.

The Real ID Act of 2005 is an \$11 billion unfunded mandate on the states.

REAL ID does need an infusion of funds, but as stated above, it is not a mandate on states. Rather, it is a long term program that requires a long term financial support plan. For now, DHS is enabling states to use up to 20% of the state's Homeland Security Grant Program funds for REAL ID. In the last grant round, roughly \$250 million was provided to states, meaning that approximately \$50 million is available for REAL ID compliance.

LAW ENFORCEMENT ACCESS TO DRIVER INFORMATION

US Law Enforcement today uses *Nlets* (International Justice & Public Safety Information Sharing Network) to exchange information regarding driver history and status for commercial and problem drivers. *Nlets* serves the law enforcement community with messaging within and between states using the Arizona Department of Public Safety facility in Phoenix. From there, all *Nlets* traffic is routed to federal, state and local law enforcement and state motor vehicle offices.

AAMVA has significantly upgraded the messaging on driver history and status by standardizing its definitions, content and format so that law enforcement personnel in any state can easily and quickly understand the data retrieved through *Nlets* as opposed to 51 varieties of data.

AAMVA based its recommendations on its CDLIS and PDPS systems, as commercial driver and problem drivers are already required to be reported between states by federal law.

The upgraded messaging system is in the process of being implemented, with a few states who have upgraded their systems – like New York, Maine and Wisconsin – already taking advantage of the uniform information now available via the AAMVA network on *Nlets*.

DHS has another \$34 million in another grant program expressly created for this purpose. However, that money will not be released until DHS submits its REAL ID implementation plan to Congress. That needs to be done promptly so seed money can be appropriately allocated for REAL ID implementation, and programs such as EVVER continue to expand. States already spending money on REAL ID implementation should be incentivized by a plan that rewards states with recovery cost money upon reaching goals set out for implementation.

States have estimated they need an initial \$1 billion in start-up costs for REAL ID, and the total costs have been estimated at around \$11 billion, although those living with the numbers think that such figures may be over-stated. More funding

is absolutely required. The \$300 million recently authorized by the House Homeland Security Committee is a good start, and momentum for funding should be encouraged.

**PUBLIC SAFETY
VALUE—BEYOND REAL
ID COMPLIANCE**

Alabama makes about 5,000 arrests per year amongst DMV applicants. DL inspectors are trained in fraud and conduct background and security checks for applicants.

Reasons include outstanding warrants, criminal charges such as murder or escape, and expired green cards. Texas and Connecticut also do such checks.

Rules for implementing the Real ID Act of 2005 have not yet been promulgated by the federal government.

The NPRM is out and comments are being solicited by DHS. States and other interests with concerns need to be responsive in a timely manner so that DHS be able to issue the final rules by the end of summer 2007. Every state has been proactive in securing their DL/ID issuance processes, and each step they take brings them closer to complying with the letter and spirit of REAL ID. States and jurisdictions with strong commitment include – but certainly are not limited to – Alabama, California, Colorado, Massachusetts, Michigan, New York, Washington and Washington D.C. Many other states are planning system enhancements that will be rolled out in the next year. And for states that are further behind, the draft rules allow states to

obtain extensions for compliance until December 31, 2009. However, all licenses and IDs held by individuals must be converted to REAL IDs by May 10, 2013 if a state intends to comply with REAL ID.

States are unclear as to the actual expected cost of compliance.

The NPRM comments and the final rules DHS decides to promulgate will further refine state costs for compliance. However, the expected cost of compliance was already calculated by an AAMVA survey that became the NGA/NCSSL September 2006 REAL ID Impact Study. At that time, each state was asked their current level of compliance and cost figures were drawn up as a result of those answers. States are now in a much better position to do cost estimates with the release of the NPRM on March 1, 2007.

Since the NPRM release, DHS has also released its estimates for REAL ID implementation at about \$23 billion. These costs are considered high by DHS, and are expected to be lower once the final rules are released. DHS estimates also contain large soft costs, such as wait times in DMV lines for REAL ID applicants, at \$7.9 billion. Although renewal times are staggered for state-issued IDs, the cost estimates to date condense this 'wait time' cost, thus also unfortunately exaggerating overall costs.

There are other costs included as well, including increased work load to process a REAL ID at another \$6.9 billion. While work load does vary by state, the NPRM still only requires one identity document be presented from a list of nine documents proposed by DHS. What may take more time until processes are streamlined as envisioned under REAL ID, are the enhanced security processes such as authenticating documents and validating applicant information. However, REAL ID implementation is headed towards automatic, real time queries which will be fast and effective. States like Kansas, for example, have moved from an over-the-counter system to a central issuance system and have reported a decrease in applicant processing time from 14 minutes per person to seven minutes per person.

Conclusion

Since 9/11, every state has sought to improve its DL/ID issuance processes. Many states are quietly working towards compliance, but all have reason to comply as REAL ID is built on the familiar turf of AAMVA's long and credible history in best practices; interoperability and exchange of information between and within states using AAMVAnet; and its long relationship with the federal government in shaping legislation such as became REAL ID. While concerns over privacy and constitutional issues have emerged and will continue to be

taken into consideration, these concerns that have not been borne out by the reality of the actual implementation taking place to date.

Perhaps the only real concern that is unanswerable at this time is cost. However, the \$300 million authorized recently in the House is a good start, and one that needs to be replicated elsewhere in Congress. We are already far out from 9/11 without a secure DL/ID issuance system in place. The longer Congress delays funding, the more difficult it will be for states to comply in a timely manner. The one billion dollars the states requested prior to the NRPM is a good place to start – with DHS estimated costs similar – in thinking about what it will take to apportion cost fairly amongst states, taking into consideration and not penalizing those states already spending their own monies for compliance.

Yet one thing is clear: we cannot afford to undo 9/11 Commission recommendations nor the good work the states have done to date to upgrade their systems. REAL ID puts the foundation in place to grow this good work by putting in place common sense standards and best practices in a reasonable, fair way that respects both the needs and limitations of both the federal and state governments.

Letter to Majority Leader Reid on REAL ID Act

02/23/2007

21 February 2007

The Honorable Harry Reid
Majority Leader
United States Senate
Washington, DC 20510

Dear Senator Reid,

I am writing on behalf of the members of the Fraternal Order of Police to advise you of our strong opposition to any amendment to S. 4, the "Improving America's Security by Implementing Unfinished Recommendations of the 9/11 Commission Act," which would repeal or otherwise negatively impact the implementation of the REAL ID Act.

The Act, which was signed into law in May 2005, establishes standards that States must meet in order for their driver's licenses and identification cards to be accepted as valid by Federal agencies. These requirements include prohibiting the issuance of a driver's license to any individual who cannot prove they are in the United States legally and prohibiting the acceptance of unverifiable foreign identification documents such as the Mexican matricula consular. The legislation authorizes a grant program to assist States in reaching these minimum standards, and would require any State that receives these grants to allow access by other States to their motor vehicle database, which will help to prevent terrorists or other criminals from obtaining multiple driver's licenses from different States. The bill also amends the Federal criminal code to prohibit trafficking in actual as well as false authentication features for use in false identification documents.

This legislation does not infringe on the privacy rights of any U.S. citizen, nor is it a "national identification card," nor does it create a national database of drivers' licenses. In fact, the model used by the REAL ID Act already exists for commercial drivers' licenses (CDLs). It is a common sense system that takes the right approach to ensuring the security and authenticity of the most commonly used identity document in the United States—a drivers' license.

For the F.O.P., this is very much an officer safety issue. Law enforcement officers need to have confidence that the documents presented to them to establish the identity of a given individual are accurate. Officers rely on these documents during traffic stops and other law enforcement actions to access information related to that individual's criminal history. No police officer wants to be in the dark about the fact that he may have detained a wanted and violent criminal who has simply obtained false identification. This places

Page 33 of 34

both the officer and the public he is sworn to protect in greater danger. For this reason, the FOP will strongly oppose any bill or amendment that would repeal the REAL ID Act.

The FOP is also very concerned about legislation or potential amendments which would further delay the implementation of the REAL ID Act. While the FOP is frustrated that the U.S. Department of Homeland Security (DHS) has not yet issued implementing regulations, many States are already well on their way to complying with the Act. Further, the DHS Secretary already has the authority to grant extensions to States which provide a reasonable justification as to why they cannot comply by the statutory deadline.

Further, the FOP is also opposed to the creation of a "negotiated rulemaking committee" to review specific factors when the DHS implementation regulations are released for public comment. We do not believe that Congress should require the formation of a special interest committee to review the regulations. Any and all parties are able to comment on the proposed rules during the public comment period. The States have an obligation and the right to identify their residents and their representatives, along with stakeholder groups like the FOP, have been meeting with DHS officials to provide ongoing feedback to the Department. We see no compelling reason why certain groups and not others should be selected and then compelled to review proposed rules based on certain factors.

The FOP supports the passage of S. 4, but we will be unable to maintain that support if the Senate adopts amendments which would repeal, or otherwise substantially weaken the REAL ID Act, which we believe will help to ensure that State-issued drivers' licenses can be counted on by the cop on the beat to identify accurately anyone with whom they may come into contact.

I want to thank you for your consideration of the views of the more than 325,000 members of the FOP on this very important issue. If I can be of any further help, please do not hesitate to contact me or Executive Director Jim Pasco in my Washington office.

Sincerely,

Chuck Canterbury
National President

cc: The Honorable Mitch McConnell, Minority Leader, U.S. Senate
The Honorable Joseph I. Lieberman, Chairman, Senate Committee on
Homeland Security and Governmental Affairs
The Honorable Susan M. Collins, Ranking Member, Chairman, Senate

Page 34 of 34

Committee on Homeland Security and Governmental Affairs

Statement
United States Senate Committee on the Judiciary
Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns
 May 8, 2007

The Honorable Patrick Leahy
 United States Senator , Vermont

Statement of Senator Patrick Leahy,
 Chairman, Senate Judiciary Committee
 “Will REAL ID Actually Make Us Safer?
 An Examination of Privacy and Civil Liberties Concerns”
 Tuesday, May 8, 2007

Today the Committee turns its attention to an issue of great concern to many States, and to Americans who value their privacy in the face of the Federal government’s expanding role in their daily lives. I thank our witnesses for being here today. I am especially pleased to welcome Allen Gilbert from Vermont.

I look forward to gaining a better understanding of the impact of the so-called REAL ID Act — an assessment that Congress should have done before this bill was passed. As we approach the second anniversary of its enactment, it is time for the Congress to come to grips with this significant policy.

The REAL ID Act was legislation forced through by the Republican Congress as an add-on to the emergency supplemental bill passed in May 2005. I do not recall hearing objection to this sweeping substantive legislation being jammed into an emergency supplemental from those who this year were so critical of the important aspects of the U.S. Troop Readiness, Veterans’ Care, Katrina Recovery, and Iraq Accountability Appropriations Act. This bill would have provided for veterans care and Katrina relief and other needs in the emergency supplemental legislation that Congress passed but the President vetoed last week.

The REAL ID Act was attached to a must-pass appropriations bill without Senate hearings or debate. Yet the implications of the Act are enormous. The Federal government will be dictating how the States go about the business of licensing residents to operate motor vehicle. State motor vehicle officials will be required to verify the legal status of applicants, adding to the responsibilities of already heavily burdened State offices. While the Federal government dictates responsibilities for what has traditionally been a State function — and adding layers of bureaucracy and regulation to effectively create a national identification card — there is no help in footing these hefty bills. Thus, in addition to privacy and civil liberties concerns, this Act is an unfunded mandate that could cost the States in excess of \$23 billion. The REAL ID Act imposes costs and Federal responsibilities on State officers.

Many States, including Vermont, have expressed their concern about the mandates of the REAL ID Act by enacting resolutions in opposition. Maine and Montana have gone so far as to indicate that they intend to refuse compliance with it. The National Conference of State Legislatures and the National Governors Association have expressed concerns about the costs imposed on the States. Opposition spans the political spectrum, from the right to the left.

The Wall Street Journal noted in an editorial that “Real Id was always more about harassing Mexican illegals than stopping Islamic terrorists” and continued to explain how “in an effort to placate noisy anti-immigration conservatives amid the GOP’s poll-driven election panic,” the Republican House in

the last Congress attached this REAL ID bill onto a “must-pass military spending bill without hearings or much debate, and Mr. Bush made the mistake of signing it.” That is from the Wall Street Journal.

Given my own concerns, I have joined with Senators Akaka, Sununu, and Tester to introduce a bill that would repeal the driver’s license provisions of the REAL ID Act, and replace those provisions with the negotiated rulemaking provisions of the Intelligence Reform Act of 2004. Senator Collins introduced a similar bill to direct the Secretary of Homeland Security to reconstitute the rulemaking committee established by the 9/11 Commission Implementation Act, a bill that she managed through Senate consideration when she chaired the Homeland Security Committee.

In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act and set up a process of negotiated rulemaking between the States and the Federal government to create minimum standards to improve the security of State-issued driver’s licenses. This process provided for the States to play an active and equal role in developing greater security measures, and to ensure that privacy concerns were addressed. This process was underway at the time the REAL ID Act passed and halted progress. Those negotiations would likely have been completed and we would already have stronger requirements for identification documents by now had the REAL ID Act not been forced through.

All Americans recognize the critical importance of national security. But for national security measures to be effective, they have to be smart as well as tough. Forcing our States to bend to the Federal will in this area may not be as effective a strategy as engaging in a cooperative process intended to serve a common goal. The reaction to the unfunded mandates of the REAL ID Act is a pretty good example of what happens when the Federal government imposes itself rather than working to create cooperation and partnership.

There are also civil liberties concerns involving this hasty Act. Americans deeply value their privacy. Americans have traditionally recognized the danger of an overreaching government. When Americans put their trust in the Federal government to exercise the immense powers conferred by the PATRIOT Act, only to see that trust terribly abused, it shakes the confidence of all Americans in a government sworn to uphold the Constitution and the rule of law.

I note, too, that today is the day that comments on the proposed REAL ID regulations are due to the Department of Homeland Security. In addition to the numerous stakeholders that I understand have made substantial comments, I hope that the DHS will pay close attention to the sentiments expressed by members of this Committee and by the Homeland Security and Government Affairs Committee, which held an oversight hearing on REAL ID in March. The days of Congress rubberstamping any and every idea cooked up by this Administration are over. We need to see real solutions with demonstrable results before we just throw away billions of dollars – or more accurately push those costs onto the States – in the name of some vague claims of enhanced security.

I look forward to hearing from our witnesses so the Committee can better understand the implications for individual privacy rights and national security of this law.

#####



STATE OF DELAWARE
OFFICE OF THE GOVERNOR

RUTH ANN MINNER
GOVERNOR

May 2, 2007

The Honorable Michael Chertoff
Secretary
Department of Homeland Security
Washington, D.C.

Attn: NAC 1-12037

Dear Secretary Chertoff:

The security and well-being of the citizens of Delaware are of paramount importance to me as Governor. Since 2001, I have worked to establish and fund critical programs and good government practices aimed at ensuring that our citizens are safe, healthy and educated. The success of many of these programs requires a strong partnership between the State and federal government, as well as tough spending decisions. As you finalize regulations to implement the REAL ID Act, I respectfully request that you consider workable solutions to key challenges posed by the Act: funding, deadlines, flexibility and citizen impacts. Further, I request that these comments be included in the official public record (DHS docket number DHS-2006-0030).

I am committed to the security and integrity of Delaware's drivers' licenses (DLs) and identification cards (IDs). In fact, over the past few years the Delaware Division of Motor Vehicles has spent approximately \$5 million in State and federal funds to increase the security of these documents. Improvements included upgrading systems, document imaging, commercial driver's license hazardous materials background checks and fingerprint capturing, capture and retention of social security numbers, security enhancements and verification of certain documents. Some of the upgrades are expected to be compliant with REAL ID but certainly not all.

Imposition of new federal mandates requires an infusion of federal funding to states through a new grant program. If federal funding is not provided to implement this federal regulation, I am greatly concerned with the length of time it will take to obtain

05/02/2007 16:26

2026245495

STATE OF DELAWARE

PAGE 03

Secretary Chertoff

May 2, 2007

Page Two

State funding to fill the gap and comply with the law. The \$3.96 million annual operating budget for Delaware DMV's Driver Services is woefully short of the estimated \$18 million in REAL ID start-up costs and even short of the \$5 million in estimated annual REAL ID operating costs to Delaware. While I realize that it is the responsibility of Congress to appropriate federal funding, the Department of Homeland Security (DHS) should request that federal grants to states be included in the President's annual budget request. Funding should not be allocated from other homeland security grant programs critical to our first responders and should not solely be paid for through increasing fees.

Lack of federal funding for implementation is compounded by the aggressive timelines for states to become compliant with the Act and ensure all DLs and IDs conform by the 2013 deadline. DHS has worked since May 2005 to release the regulations, leaving states with little time to understand the mandate, pass new state laws, find adequate funding, implement necessary changes and educate the public. All of these actions are aside from the federal requirements to establish the required electronic verification databases. Even with the extension through December 2009, implementation will be difficult to accomplish.

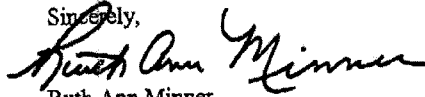
To minimize the impact on citizens, the following measures should be detailed in the final regulations. States should be allowed five years from their certification date to reissue all DL/IDs. States should not have to come into compliance with REAL ID until the electronic databases are established, filled with the necessary data and properly working to verify documents. If DHS chooses to mandate that states comply with REAL ID while the databases are still being established, then DHS must detail in the final regulations a process by which states can still be in compliance by verifying documents in another manner.

Flexibility is another key factor to the success of implementing REAL ID. The goal of REAL ID should be to establish base minimums for security of these documents and the processes by which they are fabricated. I appreciate the draft regulations provided states with flexibility in designing systems and documents appropriate to their state. I am hopeful that DHS will retain flexibility in the final regulations.

Of greatest concern to me is the real impact on the citizens of Delaware who are attempting to abide by State and federal statutes to lawfully operate a vehicle, travel and conduct business. REAL ID will greatly impact the 622,000 Delawareans holding DLs and 113,000 holding IDs. How great will the impact be and how much will our citizens be willing to endure? Those answers we don't know. However, our analysis shows that customer waiting times will increase substantially and increased costs to obtain a DL/ID will become the reality.

We will do our part to ensure the integrity of Delaware's drivers' licenses and identification cards. We anticipate the need to increase the number of employees by approximately 31 to staff the DMV counters and a new Help Desk specializing in customer service, causing DMV to modify and expand its existing facilities to accommodate the new staff. We will consider changes to the necessary State laws. And we will explain to our citizens the federal mandate placed on all of us. But the federal government needs to do its part as well. Providing federal funding, establishing all databases, identifying workable deadlines and providing states with flexibility will assist Delaware in complying with this federal mandate and lessening the drastic impacts on our citizens.

Sincerely,



Ruth Ann Minner
Governor

cc: Senator Joseph Biden
Senator Thomas Carper
Congressman Michael Castle

Testimony of Bruce Schneier

Security technologist, author, founder and CTO of BT Counterpane

“Will REAL ID Actually Make Us Safer?
An Examination of Privacy and Civil Liberties Concerns”

Senate Judiciary Committee

Room 226, Dirksen Senate Office Building

Tuesday, May 8, 2007

STATEMENT

I appreciate the opportunity to appear before the Committee today to discuss privacy issues. My name is Bruce Schneier. I am a security technologist, author, and CTO of BT Counterpane. The expertise I bring to this committee is less in the privacy and civil liberties realms, and more in the security realm. As such, I will focus my comments on the insecurities of the REAL ID system, the ineffectiveness of identity-based security systems, and the need to find smart and effective solutions to new security challenges. I'd like to emphasize at the start that this is an enormously interesting, important, and subtle topic, and I appreciate the decision of the Committee to hold these hearings.

The Electronic Privacy Information Center has coordinated comments to the Department of Homeland Security on REAL ID: signed by 21 experts on privacy and technology, including myself. I ask to submit it for the record.

When most people think of ID cards, they think of a small plastic card containing their name and a photograph. This isn't wrong, but it's only a small piece of any ID program. What starts out as a seemingly simple security device—a card that binds a photograph with a name—rapidly becomes a complex security system.

It doesn't really matter how well a REAL ID works when used by the hundreds of millions of honest people who would carry it. What matters is how the system might fail when used by someone intent on subverting that system: how it fails naturally, how it can be made to fail, and how failures might be exploited.

The first problem is the card itself. No matter how unforgeable we make it, it will be forged. The new U.S. \$20 bill was forged even before it was released to the public. We can raise the price of forgery, but we can't make it impossible. REAL IDs will be forged. And, as I will show below, the fact that a REAL ID is a more valuable identification document than a driver's license means that it is more likely to be forged.

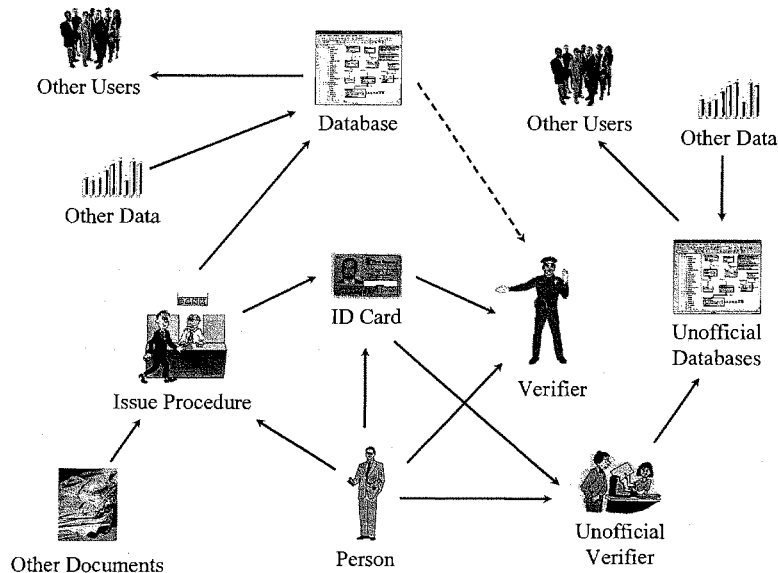
Even worse, REAL ID will not prevent people from getting legitimate cards in fraudulent names. Three of the 9/11 terrorists had valid Virginia driver's licenses in fake names, after bribing a DMV clerk. And even if we could guarantee that everyone who issued national ID cards couldn't be bribed, cards are issued based on other identity documents—all of which are easier to forge. REAL ID can be no more secure than the documents sufficient to get one.

And we can't assume that everyone will always have a REAL ID. Currently, about 20% of all identity documents are lost per year. An entirely separate security system would have to be developed for people who lost their card, a system that itself would be susceptible to abuse.

Additionally, any ID system involves people: fallible people who regularly make mistakes. We've all heard stories of bartenders falling for obviously fake IDs, or sloppy ID checks at airports and government buildings. It's not simply a matter of training; checking IDs is a mind-numbingly boring task, one that is guaranteed to have failures. The anti-counterfeiting features of REAL ID are only as good as the verification mechanisms.

All of these problems demonstrate that identification checks based on REAL ID won't be nearly as secure as we might hope. But the main problem with any strong identification system is that it requires the existence of a massive database. DHS maintains that it's not one database, but fifty-plus separate databases. This is a semantic dodge; a series of interconnected physical databases is the same as a single massive database. In this case it's a massive database of private and sensitive information on every American—one widely and instantaneously accessible from airline check-in stations, police cars, schools, and so on.

The security risks of this database are enormous. It would be a kludge of existing databases that are incompatible, full of erroneous data, and unreliable. Computer scientists don't know how to



keep a database of this magnitude secure. The daily stories we see about leaked personal information demonstrate that we do not know how to secure these large databases against outsiders, to say nothing of the tens of thousands of insiders authorized to access it. The fact that REAL ID database is a “one stop shop” for personal information exacerbates these risks.

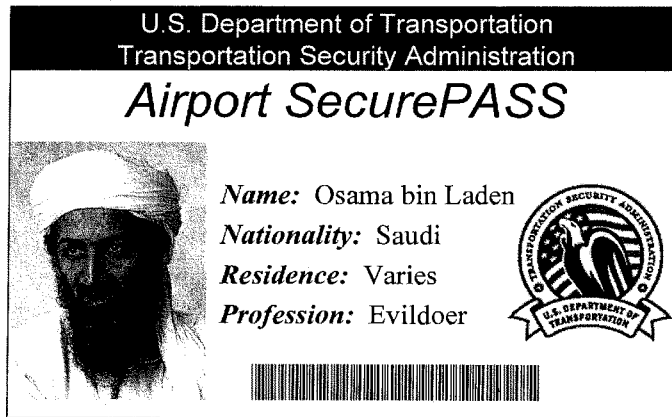
Even worse, the residential-address requirement puts domestic violence survivors at risk, both by printing the information on the card and including it in the broadly accessible database.

REAL ID creates huge risks for privacy and security. Yet DHS has punted on privacy. The agency claims it doesn’t have the power to require strong privacy protections, because the REAL ID Act did not explicitly say “DHS must set strong privacy protections for this massive trove of personal data.” It is ludicrous for the DHS to suggest that it must be explicitly told to protect the personal information of Americans. DHS has an obligation to protect citizens, and cannot shirk that obligation.

But even if we could solve all these problems, we still wouldn’t be getting very much security. A reliance on ID cards is based on a dangerous security myth, the idea that if only we knew who everyone was, we could pick the bad guys out of the crowd.

In an ideal world, what we would want is some kind of ID that denoted intention. We’d want all terrorists to carry a card that said “evildoer” and everyone else to carry a card that said “honest person who won’t try to hijack or blow up anything.” Then security would be easy. We could just look at people’s IDs, and, if they were evildoers, we wouldn’t let them on the airplane or into the building.

This is, of course, ridiculous; so we rely on identity as a substitute. In theory, if we know who you are, and if we have enough information about you, we can somehow predict whether you’re likely to be an evildoer. But that’s almost as ridiculous. If you need any evidence of this, look at the single largest identity-based anti-terrorism security measure in this country: the No-Fly List. The No-Fly List has been a disaster in every way: it harasses innocents, it doesn’t catch anyone guilty, and it is trivially easy to evade. This is what you get with identity-based security, and this is what you should expect more of with REAL ID.



Even worse, as soon as you divide people into two categories—more trusted and less trusted people—you create a third, and very dangerous, category: untrustworthy people whom we have no reason to mistrust. Oklahoma City bomber Timothy McVeigh; the Washington, DC, snipers; the London subway bombers; and many of the 9/11 terrorists had no previous links to terrorism. Evil-doers can also steal the identity—and profile—of an honest person. And if you think it's bad for a criminal to impersonate you to your bank, just wait until a terrorist impersonates you to the TSA. Profiling can result in less security by giving certain people an easy way to skirt security.

Even if you could magically solve all of these problems, REAL ID would not have prevented 9/11. Three 9/11 terrorists used legitimate driver's licenses in fake names received by bribing a Virginia DMV clerk, something REAL ID would not prevent. Some used foreign passports, something that would not be prevented by REAL ID. And it makes no sense to focus on the particular tactics of the 9/11 terrorists when there were equally effective alternate tactics. Today, it is trivially easy to fly under someone else's name. Today—and forever in the future—anyone can fly without an ID.

Enough of terrorism; what about more mundane concerns like identity theft? Perversely, a hard-to-forge ID card can actually increase the risk of identity theft. A single ubiquitous ID card will be trusted more and used in more applications. Therefore, someone who does manage to forge one—or get one issued in someone else's name—can commit much more fraud with it. A centralized ID system is a far greater security risk than a decentralized one with various organizations issuing ID cards according to their own rules for their own purposes.

Security is always a trade-off; it must be balanced with the cost. We all do this intuitively. Few of us walk around wearing bulletproof vests. It's not because they're ineffective, it's because for most of us the trade-off isn't worth it. It's not worth the cost, the inconvenience, or the loss of fashion sense. If we were living in a war-torn country like Iraq, we might make a different trade-off.

Real ID is another lousy security trade-off. The last cost estimate I saw was \$20 billion—and that makes unrealistic assumptions about IT projects being able to stay in budget—and we won't get much security in return. My recommendation is to scrap REAL ID altogether. For the price, we're not getting anywhere near the security we should.

Thank you for allowing me to address the committee. I welcome your questions.

7 May 2007

Honorable Senator Patrick Leahy
433 Russell Senate Office Building
Washington, DC 20510

Dear Senator Leahy:

Thank you for the opportunity to comment in writing on the impacts of Real ID on Vermont citizens and the Department of Motor Vehicles.

In principle, we support the intent of the Real ID and the attempt to secure our Homeland. However, the Act and proposed rules as written will pose some difficult challenges for Vermont.

There are several sections of the Act and its proposed Rules that Vermont is in compliance with. Those include legal presence requirement, residency requirement, many of the document standards, digital image on photos, document retention requirements, verification of Social Security number, etc.

The major issues for Vermont will be the reenrollment of all licensed drivers and identification card holders, lack of funding, and the timeframe for implementation.

The reenrollment requirement is extremely onerous in that it requires virtually every citizen who holds a driver's license or identification card to present documents once again to prove their identity. It will be a burden on our citizens to obtain these documents if they do not have them, as well as a burden to the vital records keepers and the Department of Motor Vehicles in requiring and verifying their authenticity. The time period for processing everyone through the system has been compressed in the proposed Rules to three years. Vermont currently has a four-year renewal cycle. Additional staff, equipment and physical space will be needed to accommodate the additional customers being served during the compressed time frame.

Funding is of great concern to Vermont. Our cost estimates originally were based on the Act itself as the proposed Rules did not come out for two years. After the proposed Rules were released, an analysis of the requirements increased the original \$2 million estimate to over \$8.5 million for Vermont to implement the Real ID Act. As you are aware, there is no funding provided to implement this Act from the Federal Government. This is a

tremendous burden to Vermont, and funding will have to be identified and passed on to the citizens of the State.

While some provisions of the Rule are not specific, they do imply some changes in how Vermont does business and serves its citizens. Specifically, the security requirements lead to the assumption that we will have to move from an over-the-counter service delivery model to a central issue of our driver license and identification cards. Over the past several years, our Department has made great strides in improving its level of service by providing more services closer to those we serve. This has been due in large part through the expansion of services that we provide at our branch offices. This level of service will change with central issue.

The requirements for financial and background checks on existing employees of the department will be an additional burden. There will be a cost to do these checks as well as the real likelihood that this will lead to the displacement of long-term, productive employees with no history of problems in the workplace. The financial check is also an invasion of the employee's privacy for purposes of "information" only.

The proposed Rules also imply that in the future each state will be forced to move to a common card stock and security features for all driver's licenses and identification cards. The implied new document is one that is currently not used by Vermont or any other state, and would greatly increase the costs to Vermont. The use of the same card stock by all states could also increase the opportunity to produce fraudulent Vermont documents once any other state's documents have been compromised.

A concern that Vermont has in the language that speaks to use of these documents and the intended "official purpose" is that it allows the Secretary of DHS to expand that definition at his discretion. Currently, the defined "official purpose" is accessing federal facilities, boarding federally-regulated commercial aircraft, and entering nuclear power plants. If that list were to expand, we would urge state input.

A concern for Vermont law enforcement is the possibility of the information on the machine-readable portion of the license being encrypted. Recently, law enforcement has begun to use the license's machine-readable portion as a field tool for various reasons such a verification and saving time writing tickets. There are also other legitimate and valuable uses of this technology. For example, retailers have found readers to verify the information in the machine-readable portion of the license to be an effective tool to verify the identity and legal age of people purchasing alcohol and tobacco.

Vermont recognizes the importance of privacy and confidentiality of information and the protection of customer information. Vermont follows the Drivers Privacy Protection Act (DPPA). We are very interested in the development, governance and protection of the data and information of the "federal reference" databases, not only from the privacy point of view but also the level of effort and cost to the State.

In conclusion, the Vermont Department of Motor Vehicles has been issuing drivers licenses to its citizens for over 75 years, for the primary purpose of attesting to a person's ability to drive and safety reasons. Over the years our core business has changed due to federal mandates, state legislative initiatives, and ancillary requirements. These changes have led to the driver's license and identification cards being one of the most commonly accepted forms of identification in the United States. The requirements in the Real ID Act will now make the driver's license and identification card issued by the states the primary form of identification nationwide.

Vermont remains committed to increasing the security and integrity of the process by which we issue our driver's license and identification cards. However, we feel that many of the Real ID Act's requirements are unnecessarily burdensome to both our citizens and the departments required to implement them, with no practical benefit.

Once again, thank you for the opportunity to comment on the behalf of the Vermont Department of Motor Vehicles.

Very truly yours,

Bonnie L. Rutledge
Commissioner

National ID Party
Wall Street Journal
February 17, 2005

Republicans swept to power in Congress 10 years ago championing state prerogatives, and one of their first acts was to repeal federal speed-limit requirements. Another was aimed at ending unfunded state mandates. So last week's House vote to require costly and intrusive federal standards for state drivers' licenses is a measure of how far the party has strayed from these federalist principles.

More important, it reveals a mindset among some that more enforcement alone will bring better border security and reduce illegal immigration. The bill that passed the House last week and now goes to the Senate is known as the **Real ID Act**, and the driver's license requirements may not even be the worst part of the legislation. Also included are unnecessary provisions that would make it much more difficult for foreigners to seek asylum in the U.S.

House Judiciary Chairman James Sensenbrenner, who authored the bill, insists that his goal is to reduce the terrorist threat, not immigration. But it just so happens that the bill's provisions have long occupied the wish list of anti-immigration lawmakers and activists. Mr. Sensenbrenner produced a photo of Mohammed Atta during the floor debate last week, arguing that the 9/11 hijackers' ability to obtain drivers' licenses and use them to board airplanes represents a security loophole.

His solution is to force states to issue federally approved drivers' licenses with digital photographs and "machine-readable technology." In theory, states can opt out, but if they do their drivers' licenses will no longer be accepted as identification to board planes, purchase guns, enter federal buildings and so forth. It's not hard to imagine these de facto national ID cards turning into a kind of domestic passport that U.S. citizens would be asked to produce for everyday commercial and financial tasks.

Aside from the privacy implications of this show-us-your-papers Sensenbrenner approach, and the fact that governors, state legislatures and motor vehicle departments have denounced the bill as expensive and burdensome, there's another reality: Even if the **Real ID Act** had been in place prior to 9/11, it's unlikely that the license provisions would have prevented the attacks.

That's because all of the hijackers entered the U.S. legally, which means they qualified for drivers' licenses. The **Real ID Act** wouldn't change that. Moreover, you don't need a driver's license to fly. Other forms of identification -- such as a passport -- are acceptable and also were available to the hijackers. Nothing in the Sensenbrenner bill would change that, either.

The biggest impact will be on undocumented workers in the U.S., which is why the immigration restrictionists are pushing for the legislation. But denying drivers' licenses to illegal aliens won't result in fewer immigrants. It will result in more immigrants driving illegally and without insurance.

Mr. Sensenbrenner's claims that tougher asylum provisions will make us safer are also dubious. The last thing a terrorist would want to do is apply for asylum. Not only would he be bringing himself to the attention of the U.S. government -- the first step is being fingerprinted -- but the screening process for applicants is more rigorous than for just about anyone else trying to enter the country. In the past decade, perhaps a half-dozen individuals with some kind of terrorists ties have applied for asylum. All were rejected.

The **Real ID Act** would raise the bar substantially for granting asylum to people fleeing persecution. But this is a solution in search of a problem. A decade ago the U.S. asylum laws were in fact being abused by foreigners with weak claims who knew they would receive work permits while their cases were pending.

But in 1994, the Clinton Administration issued regulations to curb this abuse. The law now says that asylum seekers cannot receive work permits until they have won their case. Applications per year

subsequently have fallen to about 30,000 today from 140,000 in the early 1990s. This was the biggest abuse of the system, and it's been fixed. Raising the barrier for asylum seekers at this point would only increase the likelihood of turning away the truly persecuted.

But the bigger problem with Mr. Sensenbrenner's bill is that it takes our eye off the ball. Homeland security is about taking useful steps to prevent another attack. It's not about keeping gainfully employed Mexican illegals from driving to work, or cracking down on the imagined hordes gaming our asylum system.

President Bush realizes this and is pushing for a guest-worker program that would help separate people in search of employment from potential terrorists. If the Republican Congress doesn't realize that, perhaps a Presidential veto of the **Real ID** Act would focus its attention.

Immigration Reality Check
Wall Street Journal
May 4, 2005

'Seal the border' populists on cable news and talk radio maintain that anti-immigrant sentiment in the U.S. is ascendant. But a recent Senate vote shows more support for the type of guest-worker initiative that President Bush proposes. Economic reality bites -- even in Congress.

Last month 53 Senators voted for a temporary-visa program to address labor demands in the agriculture industry. And while that was fewer than the 60 votes needed to add the measure to an Iraq spending bill, it does indicate a recognition by a majority of Senators that enforcement-only approaches to illegal immigration won't work.

The farm-worker legislation, sponsored by Idaho Republican Larry Craig and known as AgJobs, has two main components. First, it would overhaul the existing H-2A visa program by streamlining an impractical and cumbersome bureaucratic hiring process that invites noncompliance. To wit, somewhere between one-half and three-quarters of the U.S. agriculture workforce is illegal.

Second, AgJobs would give those illegal aliens who can pass a background check and demonstrate an employment history the opportunity to continue working here under a temporary status and ultimately earn a green card. This approach is branded an "amnesty" and therefore dismissed out of hand by conservative opponents of AgJobs. Not that these critics are proposing any viable alternatives.

As a political matter there's no majority support -- bipartisan or otherwise -- for any immigration reform that doesn't realistically address the illegal aliens already here. A counterproposal considered by the Senate that would have required undocumented workers to return home to apply for legal status garnered all of 21 votes.

Moreover, the Senate floor debate made it clear that there's a real world demand for immigrant workers if U.S. agriculture is going to remain productive and competitive. Senator George Voinovich of Ohio, where agribusiness contributes \$73 billion a year to the economy, told fellow Members that AgJobs reforms are necessary for the industry to stay strong and vibrant.

Mr. Voinovich also described how flexible labor markets can operate to everyone's advantage. "Agricultural economists tell us each farmworker job in these [fruit, vegetable, nursery crops] industries supports 3 1/2 jobs in the surrounding economy: processing, packaging, transportation, equipment, supplies, lending, and insurance," said the Senator. "They are good jobs, filled by Americans. We lose them if we do not do this the right way."

President Bush believes the "right way" is a guest-worker program not only for agriculture but other industries as well. But restrictionists continue to insist that illegal immigration can be stopped through enforcement measures alone, such as those in the **REAL ID** Act that passed the House in March and is now being considered by Congress as part of the supplemental spending bill.

Among other things, illegal immigrants would be denied drivers' licenses under **REAL ID**, and asylum seekers would face greater scrutiny. Last week, the White House lent its support to the bill in hopes of receiving some reciprocal cooperation for its guest-worker initiative. We understand the strategy, but the asylum measures are unnecessary given reforms of the mid-1990s. As for licenses, applying for one is an act of trying to obey the law; denying them will merely cause immigrants to drive unlicensed and uninsured. The spectacle of a GOP Congress imposing this unfunded mandate on the states is also embarrassing; what's next, a return of the 55 mile-per-hour national speed limit?

So long as the U.S. shares a 2,000-mile border with a developing nation, we'll never reduce the illegal flow with punitive measures that ignore the market forces luring foreign workers here in the first place.

The best way to decrease the number of illegal crossings, while also satisfying our economic needs, is to give immigrants more legal ways to come. Under the World War II-era bracero program, which allowed Mexican workers entry to meet the labor demands of American growers, illegal border crossings fell.

The U.S. border-enforcement budget has quintupled since 1993 -- one of the highest growth rates in the federal government after defense spending. Yet the illegal immigrant population in the U.S. has continued to increase. Readers may remember the days when conservatives criticized liberals for throwing money at policies that aren't working.

With its majority Senate support, the AgJobs bill is a sign that Mr. Bush's guest-worker idea isn't as dead as advertised by the anti-immigration right. It deserves to be considered as a stand-alone measure, and the sooner the better. Everyone complains about the lack of bipartisanship in Washington. But here's a case where business and labor have joined with Democrats and Republicans to address what all agree is a problem. So why not get it done?

Deputizing the DMV
Wall Street Journal
July 25, 2005

Bowing to pressure from immigration restrictionists in his Republican caucus, President Bush signed an emergency spending bill in May with an unrelated rider that denies driver's licenses to illegal aliens. But a funny thing has happened on the way to implementing the law, which effectively delegates border patrol and FBI duties to clerks at that model of speed and efficiency -- your local Department of Motor Vehicles.

At a National Governors' Association meeting in Iowa last week, Democrats and Republicans alike denounced the measure, known as the **Real ID** Act, as impractical and vastly underfunded. Republican Mike Huckabee of Arkansas said his Motor Vehicle clerks, whose pay starts at \$8.27 an hour, haven't the knowledge or skills to verify whether license applicants are legal residents of the U.S. Democrat Mark Warner of Virginia said such training could easily cost each state upward of \$100 million, or the amount Congress appropriated for all 50 states. Our guess is that these costs ultimately will be passed on to drivers in the form higher fees.

Aside from the logistical problems, however, New Mexico's Bill Richardson, another Democrat, said the law is bad policy. A licensed illegal alien is easier to keep track of. And since denying a driver's license to a person willing to risk his life to get here is unlikely to be much of a deterrent to coming, the law will do little more than increase the number of unlicensed and uninsured motorists.

The White House is hoping enforcement concessions will produce GOP support for a more ambitious immigration reform agenda that includes a guest-worker program. But so far that approach doesn't seem to be working. And in the case of **Real ID**, it's making a bad situation worse.

Real ID Revolt

Source: The Wall Street Journal

Date: 05/08/2007

Back in 2005, when Republicans ran Congress and were convinced that bashing immigration would help the party retain its majority, President Bush signed the Real ID Act. Sold as a homeland security measure, the law requires the 50 states to issue federally approved drivers licenses and link their identification databases. Two years later, a growing number of states are telling Congress what it can do with its de facto national ID card decree.

So far, seven states have enacted statutes or resolutions opposing the implementation of Real ID, and Oklahoma is on the verge of becoming the eighth. Oklahoma City and Tulsa aren't known as liberal hotbeds. Anti-Real ID measures have passed at least one chamber of legislatures in 14 states and been introduced in 11 others.

Costs and privacy concerns explain much of the opposition. A study released last year by the National Governors Association, which opposes the law, put the implementation price tag at \$11 billion. But an analysis by the Department of Homeland Security released in March concedes that the costs will be at least double that amount.

Under Real ID, which is scheduled to go into effect next year, all 245 million current license holders in the U.S. are required to head down to the local Department of Motor Vehicles with certified source documents -- such as a birth certificate or Social Security card -- to apply for the new standardized national ID. And people from states that don't play ball won't be able to use their licenses to board planes or enter federal buildings.

In California today, where a nation-high 25 million licenses are issued, residents can renew by mail. Real ID requires that you appear in person. So Americans can be grateful that DMVs nationwide are known as models of hassle-free efficiency; be sure to book a free afternoon.

Americans are rational. And in a post-9/11 world, they are willing to trade some freedom and convenience for more security. But it's not at all clear that Real ID will make us safer. Deputizing motor vehicle office clerks, who would be entrusted with sensitive information and access to a national databank, also entails considerable privacy risk.

Fraud and security lapses at DMVs today are hardly uncommon. Just last month, a DMV official in North Carolina was arrested in connection with issuing fraudulent drivers licenses. And if the goal is to stop the next Mohammed Atta, it's worth noting that, even under Real ID, people would be permitted to fly with identification other than licenses.

Real ID was always more about harassing Mexican illegals than stopping Islamic terrorists. It's true that the 9/11 Commission urged the federal government to "set

standards for the issuance . . . of sources of identification, such as drivers licenses." That's why the Intelligence Reform and Terrorism Prevention Act of 2004 included tougher identity security provisions. The law also directed the Departments of Transportation and Homeland Security to work with state officials, technology experts and privacy groups to come up with standards that balance security and civil liberties.

But in an effort to placate noisy anti-immigration conservatives amid the GOP's poll-driven election panic, then-House Judiciary Chairman James Sensenbrenner gutted those provisions and replaced them with the expensive and intrusive Real ID. For unexplained reasons, immigration restrictionists are convinced that preventing illegal aliens from obtaining drivers licenses will result in fewer illegal aliens, rather than merely more unlicensed and uninsured motorists. Mr. Sensenbrenner attached Real ID to a must-pass military spending bill without hearings or much debate, and Mr. Bush made the mistake of signing it.

In addition to the revolt in the states, legislation co-sponsored by John Sununu (R., N.H.) and Daniel Akaka (D., Hawaii) has been introduced in the Senate. Their bill would repeal the Real ID Act and return to the negotiated rulemaking process laid out in the 2004 intelligence reform bill. Senate Judiciary Chairman Pat Leahy has scheduled a hearing for today on Real ID, the kind of session that usually takes place before something becomes law. Perhaps Mr. Sensenbrenner should be invited to explain the national revolt against his handiwork.